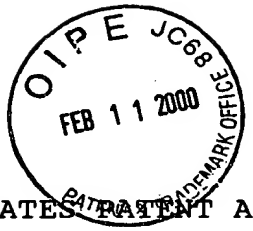
2766 #3

Priority Papers

500.38035X00

4-V
3.3.00



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): H. KURUMATANI

Serial No.: 09/468,948

Filed: December 22, 1999

Title: METHOD AND APPARATUS FOR ELLIPTIC CURVE CRYPTOGRAPHY AND RECORDING MEDIUM THEREFOR

Group:

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

February 11, 2000

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 10-364277
Filed: December 22, 1998

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/ssr
Attachment

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１２月２２日

出 願 番 号
Application Number: 平成１０年特許願第３６４２７７号

出 願 人
Applicant (s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

TIFIED COPY OF
ITY DOCUMENT

１９９９年１２月１０日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆

出証番号 出証特平１１－３０８６３７３

【書類名】　特許願

【整理番号】　K98013811

【提出日】　平成10年12月22日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

【発明の名称】　楕円曲線暗号実行方法及び装置並びに記録媒体

【請求項の数】　7

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町５０３０番地　株式会社日立製作所　ソフトウェア事業部内

【氏名】　車谷　博之

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100068504

【弁理士】

【氏名又は名称】　小川　勝男

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

出証特平１１－３０８６３７３

【書類名】　明細書

【発明の名称】　楕円曲線暗号実行方法及び装置並びに記録媒体

【特許請求の範囲】

【請求項１】

楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の加算をＰ３（ｘ３，ｙ３）とし、点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の減算をＰ４（ｘ４，ｙ４）とした場合、前記ｘ１を入力するステップと、前記入力されたｘ１を射影空間のＸ座標、Ｚ座標［X_1，Z_1］に変換するステップと、前記射影空間の座標［X_1，Z_1］を記憶するステップと、前記ｘ２を［X_2，Z_2］に変換するステップと、前記［X_2，Z_2］を記憶するステップと、前記ｘ４を［X_4，Z_4］に変換するステップと、前記［X_4，Z_4］を記憶するステップと、前記記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］から［X_3，Z_3］を求めるステップと、前記［X_3，Z_3］からｘ３に変換するステップと、前記ｘ３を出力するステップとからなり、点Ｐ１（ｘ１，ｙ１）のスカラー倍を計算することを特徴とする楕円曲線暗号実行方法。

【請求項２】

請求項１記載の楕円曲線暗号実行方法であって、乱数ｋを生成するステップと、前記生成された乱数ｋを記憶するステップと、ｘ座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数ｋと演算させて、射影座標［k^2x，ｋ］に変換するステップとを有することを特徴とする請求項１記載の楕円曲線暗号実行方法。

【請求項３】

請求項１記載の楕円曲線暗号実行方法であって、乱数ｋを生成するステップと、前記生成された乱数ｋを記憶するステップと、ｘ座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数ｋと演算させて、射影座標［ｋｘ，ｋ］に変換するステップとを有することを特徴とする請求項１記載の楕円曲線暗号実行方法。

【請求項４】

請求項１記載の楕円曲線暗号実行方法であって、記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］からｘ３に変換できる［X_3，Z_3］を求めるステップには、$B=X_1Z_2^2+X_2Z_1^2$を計算するステップと、前記計算されたＢを記憶するステップと、前記記憶されたＢをＢ＝０であるか否かをを判別するステップと、Ｂ＝０の場合は無限遠点を出力し、Ｂ＝０でない場合は$Z_3=Z_4B$を計算するステップと、前記計算されたZ_3を記憶するステップと、前記記憶されたZ_3から$X_3=X_4Z_3^2+X_1X_2Z_1^2Z_2^2Z_4^2$を計算するステップとを有することを特徴とする請求項１記載の楕円曲線暗号実行方法。

【請求項５】

請求項１記載の楕円曲線暗号実行方法であって、記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］からｘ３に変換できる［X_3，Z_3］を求めるステップには、　$B=X_1Z_2+X_2Z_1$を計算するステップと、前記計算されたＢを記憶するステップと、前記記憶されたＢをＢ＝０であるか否かをを判別するステップと、Ｂ＝０の場合は無限遠点を出力し、Ｂ＝０でない場合は$Z_3=Z_4^2B^2$及び$X_3=X_4B^2+X_1X_2Z_1Z_2Z_4^2$を計算するステップとを有することを特徴とする請求項１記載の楕円曲線暗号実行方法。

【請求項６】

楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の演算装置であって、乱数ｋを生成する乱数生成部と、２の拡大体上の座標ｘ０と前記乱数ｋとを入力し、射影座標［ｋｘ０，ｋ］＝［X_1，Z_1］に変換する射影座標変換部と、前記［X_1，Z_1］から２倍点を演算し出力する２倍演算部と、前記［X_1，Z_1］から加算点を求め出力する加算演算部と、前記射影座標変換部と前記２倍演算部と前記加算演算部からの情報を得て、座標ｘ０をスカラー倍するスカラー倍部とを有することを特徴とする楕円曲線演算装置。

【請求項７】

楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の実行方法を格納した記録媒体であって、前記楕円曲線暗号の実行方法は以下を含む：各座標成分が前記楕円曲線上の点である点Ｐ１（ｘ１，ｙ１），Ｐ２（

ｘ２，ｙ２）の加算をＰ３（ｘ３，ｙ３）とし、点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の減算をＰ４（ｘ４，ｙ４）とした場合、前記ｘ１を入力するステップと、前記入力されたｘ１を射影空間のＸ座標、Ｚ座標［X_1，Z_1］に変換するステップと、前記射影空間の座標［X_1，Z_1］を記憶するステップと、前記ｘ２を［X_2，Z_2］に変換するステップと、前記［X_2，Z_2］を記憶するステップと、前記ｘ４を［X_4，Z_4］に変換するステップと、前記［X_4，Z_4］を記憶するステップと、前記記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］から［X_3，Z_3］を求めるステップと、前記［X_3，Z_3］からｘ３に変換するステップと、前記ｘ３を出力するステップとからなり、点Ｐ１（ｘ１，ｙ１）のスカラー倍を計算する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータネットワークにおいてセキュリティを確保する技術に係り、特に楕円曲線暗号を実行する方法及び装置並びに記録媒体に関する。

【０００２】

【従来の技術】

楕円曲線暗号は、V.Miller，N.Koblitz両氏によって、独立に発明された公開鍵暗号である。公開鍵暗号技術において安全上からの要請として、他人に公開される公開鍵から、それに対応する秘密鍵を発見することが事実上不可能であることが求められる。その一方で、秘密鍵暗号方式に比べて基本的に暗号化や復号化に時間のかかる公開鍵暗号方式において、暗号化や復号化におけるより高速のものが求められている状況にある。このように、安全性と高速性という、ある意味で背反的な要請を実現する公開鍵暗号技術として、従来からのＲＳＡ暗号やエルガマル暗号に比べてより上述の性質を有する楕円曲線暗号が注目されてきている。

【０００３】

楕円曲線暗号は、有限素体上の楕円曲線の標準形$y^2=x^3+ax+b$（$4a^3+27b^2\neq 0$）や２の拡大体上の楕円曲線の標準形$y^2+xy=x^3+ax$

^{2}＋ｂ（ｂ≠０）で表される。この曲線上の点に、無限遠点を加えると、アーベル群が成立する。このアーベル群演算を＋記号で表現する。相異なるＸ，Ｙ間の演算をＸ＋Ｙを加算演算と呼ぶ。また、Ｘ＋Ｘを２倍演算と呼び、２Ｘと表現する。

【０００４】

かかる楕円曲線は、その計算を容易にするためにアフィン座標における楕円曲線上の点（Ｘ，Ｙ）を射影座標で表現することもある。任意のλ≠０について，

［Ｘ，Ｙ，Ｚ］＝　［λ^{2}Ｘ，λ^{3}Ｙ，λＺ］となる射影座標を考えると、アフィン座標とこの射影座標の対応は以下で与えられる。すなわち、アフィン座標（ｘ，ｙ）は、射影座標［ｘ，ｙ，１］で表現され、射影座標［Ｘ，Ｙ，Ｚ］は、アフィン座標（Ｘ／（Ｚ）^{2}，Ｙ／（Ｚ）^{3}　）となる。また、射影座標において－［Ｘ，Ｙ，Ｚ］＝［Ｘ，－Ｙ，Ｚ］である。

【０００５】

楕円曲線暗号は、有限体上の楕円曲線を用いて、その有限体となる点の集合を用いる。また、楕円曲線の位数は、楕円曲線の点の数である。以下、Ｐをｓ回加算（Ｐ＋Ｐ＋…＋Ｐ）した結果をＰのｓ倍点といい、これを求める演算をｓＰと書くと、楕円曲線上の点Ｐの位数は、ｎＰ＝０，１＜＝ｍ＜ｎ，ｍＰ　≠０となるｎである１１２となる。

【０００６】

楕円曲線暗号の鍵は、楕円曲線、ベースポイント、公開鍵、秘密鍵から構成され、具体的には、楕円曲線の係数ａ，ｂ、位数が素数である点Ｐ（ベースポイント）、有限体要素ｄ（秘密鍵）、ベースポイントの秘密鍵倍の点Ｑ（公開鍵：Ｑ＝ｄＰ）である。ここで、楕円曲線、ベースポイント、公開鍵は公開情報である。また、公開鍵／秘密鍵は、ユーザ毎に異なる値であり、楕円曲線、ベースポイントは、ユーザ間共通の値である。

【０００７】

楕円曲線暗号における、データ暗号化、データ復号化、ディジタル署名作成、ディジタル署名検証は、任意の点Ｒのスカラ倍ｓＲ演算を用いる。これは、上記の加算演算と２倍演算の組合せで、求めることができる。ところが、上記の加算

演算と２倍演算計算法においては、それぞれ１回の除算が必要であり、一般に有限体の除算は非常に時間がかかるため、これを避ける方法が求められる。

【０００８】

文献D.V.Chudnovsky, G.V.Chudnovsky "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, 7, 385-434,1986によれば、この有限体の除算を避けるため、射影空間で、加算演算、２倍演算の式を導出している。この場合、素体乗算と、素体加減算では素体乗算が通常、遥かに時間がかかるため、素体乗算演算数で、計算時間を評価できる。この場合、加算演算で、素体乗算（２乗算を含む）が１６回必要である。２倍演算において、１０回必要である、と述べている。また、楕円曲線の係数ａにおいても、ａ＝－３の場合、８回の乗算剰余演算となるとしている。

【０００９】

また、P.Montgomery,"Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation Vol.48,No.177,pp.243-264(1987)によれば、有限素体上の楕円曲線の標準形$By^2=x^3+Ax^2+Bx$を用いて、点Ｐ０（ｘ０，ｙ０），Ｐ１（ｘ１，ｙ１）の加算をＰ３（ｘ３，ｙ３）、減算をＰ４（ｘ４，ｙ４）、すなわちＰ１＋Ｐ０＝Ｐ３、Ｐ１－Ｐ０＝Ｐ４とするとき、ｘ０，ｘ１，ｘ４から、ｘ３が高速に求まる。具体的には、素体の乗算６回で求まるとされている。また、Ｐ１の２倍点をＰ５（ｘ５，ｙ５）とするとき、ｘ５は、ｘ１のみから求まり、乗算５回である。これを利用して、点Ｒのスカラ倍（スカラー値ｄ）のｘ座標を以下のようにＲｘから求めることができる。

【００１０】

初期値を［Ｒ，２Ｒ］、ｍＲをＲのｍ倍のｘ座標とするとき、ｄを２進数展開し、ｄの上位ビットから、０の場合は、［ｍＲ，（ｍ＋１）Ｒ］→　［２ｍＲ，（２ｍ＋１）Ｒ］となり、１の場合は、［ｍＲ，（ｍ＋１）Ｒ］→［（２ｍ＋１）Ｒ，２（ｍ＋１）Ｒ］となる。尚、（ｍ＋１）Ｒ－ｍＲ＝Ｒ、（ｍ＋１）Ｒ＋ｍＲ＝（２ｍ＋１）Ｒである。

【００１１】

従って、１ビットあたり、６＋５＝１０回の素体乗算（２乗算を含む）でスカラー倍ｓＰを求めることができる。これを以下、モンゴメリ法と呼ぶ。

【００１２】

一方、２の拡大体上の楕円曲線の標準形$y^2+xy=x^3+ax^2+b$（$b\neq 0$）で表される。このスカラー倍演算も、加算演算、２倍演算の組合せで実現できる。IEEE P1363 / D2 Standard Specification for Public Key Cryptography (1998)では、加算演算と２倍演算規則を与えている。２の拡大体演算では、２乗算、加減算は相異なる乗算に比べて非常に速く演算できるので、（相異なる）乗算回数で評価できる。加算演算で１５回の乗算、２倍演算で５回の乗算が必要となる。しかし、２の拡大体楕円曲線暗号ではモンゴメリ法を用いる演算は知られていない。

【００１３】

安全な楕円曲線とするためには、楕円曲線の位数＃Ｅ（Ｆｑ）が大きな素因数ｒを持つパラメタａ，ｂを設定する必要がある。＃Ｅ（Ｆｑ）＝ｋｒで、ｋは小さな整数、ｒは大きな素数となる。そのが位数大きな素因数を持つ楕円曲線のパラメタの設定方法は、例えば文献Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM138, Springer(1993) p.464 Atkin's Testで記述されている方法がある。

【００１４】

次に暗号のアタックと防御について述べる。近年、暗号のアタックは、理論的な暗号解読に加え、消費電流波形を統計的に処理して解読を試みるＤＰＡ(Differential Power Analysis)や暗号処理時間の違いから統計的に分析し解読を試みるタイミングアタック等、リーク情報を分析する攻撃とその防御が研究されはじめている。これらの防御研究の多くは、主にＩＣカードを分析する等のハードウェア回路そのものに防御機能を組み込むことが中心になっている。

【００１５】

【発明が解決しようとする課題】

上述したように２の拡大体の楕円曲線暗号ではモンゴメリ法を用いる演算は知

られていない。また、楕円曲線暗号の研究においては、主に高速な実行方法、暗号解読の観点からの安全な楕円曲線生成の研究開発が中心であり、リーク情報分析型のアタックに対する防御開発は行われていない。楕円曲線暗号のデータ復号化処理では、与えられた楕円曲線上の点（ｘ，ｙ）の秘密鍵ｄから、（ｘ，ｙ）のｄ倍演算ｄ（ｘ，ｙ）を行う。ｄの偏差情報を消費電流波形や暗号処理時間に洩れる場合ＤＰＡやタイミングアタックへの手がかりを与えてしまう。本発明の第１の目的は、楕円曲線が$y^2+xy=x^3+ax^2+b$（ｂ≠０）である、２の拡大体上の楕円曲線暗号を高速に演算する方法及び装置を提供することにある。また、本発明の第２の目的は、楕円曲線暗号においてタイミングアタックやＤＰＡによる攻撃を防御するための、処理時間の偏差情報から秘密鍵情報がもれない方法を提供することにある。

【００１６】

【課題を解決するための手段】

本発明の第１の目的は、楕円曲線が$y^2+xy=x^3+ax^2+b$（ｂ≠０）である、２の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の加算をＰ３（ｘ３，ｙ３）とし、点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の減算をＰ４（ｘ４，ｙ４）とした場合、前記ｘ１を入力するステップと、前記入力されたｘ１を射影空間のＸ座標、Ｚ座標$[X_1, Z_1]$に変換するステップと、前記射影空間の座標$[X_1, Z_1]$を記憶するステップと、前記ｘ２を$[X_2, Z_2]$に変換するステップと、前記$[X_2, Z_2]$を記憶するステップと、前記ｘ４を$[X_4, Z_4]$に変換するステップと、前記$[X_4, Z_4]$を記憶するステップと、前記記憶された$[X_1, Z_1]$，$[X_2, Z_2]$，$[X_4, Z_4]$から$[X_3, Z_3]$を求めるステップと、前記$[X_3, Z_3]$からｘ３に変換するステップと、前記ｘ３を出力するステップとからなり、点Ｐ１（ｘ１，ｙ１）のスカラー倍を計算することにより達成される。また、記憶された$[X_1, Z_1]$，$[X_2, Z_2]$，$[X_4, Z_4]$からｘ３に変換できる$[X_3, Z_3]$を求めるステップには、$B=X_1 Z_2^{\,2}+X_2 Z_1^{\,2}$を計算するステップと、前記計算されたＢを記憶するステップと、前記記憶されたＢをＢ＝０であるか否かをを判別するス

テップと、Ｂ＝０の場合は無限遠点を出力し、Ｂ＝０でない場合は$Z_3=Z_4B$を計算するステップと、前記計算されたZ_3を記憶するステップと、前記記憶されたZ_3から$X_3=X_4Z_3^2+X_1X_2Z_1^2Z_2^2Z_4^2$を計算するステップとを有することにより達成される。

【００１７】

本発明の第２の目的は、２の拡大体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報がもれない方法、すなわち楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の実行方法であって、各座標成分が前記楕円曲線上の点である点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の加算をＰ３（ｘ３，ｙ３）とし、点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の減算をＰ４（ｘ４，ｙ４）とした場合、前記ｘ１を入力するステップと、前記入力されたｘ１を射影空間のＸ座標、Ｚ座標［X_1，Z_1］に変換するステップと、前記射影空間の座標［X_1，Z_1］を記憶するステップと、前記ｘ２を［X_2，Z_2］に変換するステップと、前記［X_2，Z_2］を記憶するステップと、前記ｘ４を［X_4，Z_4］に変換するステップと、前記［X_4，Z_4］を記憶するステップと、前記記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］から［X_3，Z_3］を求めるステップと、前記［X_3，Z_3］からｘ３に変換するステップと、前記ｘ３を出力するステップの他、さらに乱数ｋを生成するステップと、前記生成された乱数ｋを記憶するステップと、ｘ座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数ｋと演算させて、射影座標［k^2x，ｋ］に変換するステップとを有することにより達成される。すなわち、２の拡大体の演算対象が乱数によって常に変更する方法を用いる。

【００１８】

また、乱数ｋを生成するステップと、前記生成された乱数ｋを記憶するステップと、ｘ座標を射影座標に変換した後、射影空間の各座標成分と前記記憶された乱数ｋと演算させて、射影座標［ｋｘ，ｋ］に変換するステップとを有することにより達成される。また、楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の演算装置であって、乱数ｋを生成する乱数生成部と

、２の拡大体上の座標ｘ０と前記乱数ｋとを入力し、射影座標［ｋｘ０，ｋ］＝［X_1，Z_1］に変換する射影座標変換部と、前記［X_1，Z_1］から２倍点を演算し出力する２倍演算部と、前記［X_1，Z_1］から加算点を求め出力する加算演算部と、前記射影座標変換部と前記２倍演算部と前記加算演算部からの情報を得て、座標ｘ０をスカラー倍するスカラー倍部とを有することにより達成される。

【００１９】

また、楕円曲線が$y^2+xy=x^3+ax^2+b$である、２の拡大体上の楕円曲線暗号の実行方法を格納した記録媒体であって、前記楕円曲線暗号の実行方法は以下を含むことにより達成される。すなわち、各座標成分が前記楕円曲線上の点である点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の加算をＰ３（ｘ３，ｙ３）とし、点Ｐ１（ｘ１，ｙ１），Ｐ２（ｘ２，ｙ２）の減算をＰ４（ｘ４，ｙ４）とした場合、前記ｘ１を入力するステップと、前記入力されたｘ１を射影空間のＸ座標、Ｚ座標［X_1，Z_1］に変換するステップと、前記射影空間の座標［X_1，Z_1］を記憶するステップと、前記ｘ２を［X_2，Z_2］に変換するステップと、前記［X_2，Z_2］を記憶するステップと、前記ｘ４を［X_4，Z_4］に変換するステップと、前記［X_4，Z_4］を記憶するステップと、前記記憶された［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］から［X_3，Z_3］を求めるステップと、前記［X_3，Z_3］からｘ３に変換するステップと、前記ｘ３を出力するステップとからなり、点Ｐ１（ｘ１，ｙ１）のスカラー倍を計算する。

【００２０】

また、上述した２の拡大体上の楕円曲線暗号の実行方法は、素体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報がもれない方法としても適用可能である。素体上の楕円曲線暗号において、上記課題（２）を解決するため、次の（ａ），（ｂ）を組合わせる。次の（ａ），（ｂ）を組合わせる。（ａ）楕円曲線のスカラー倍ｄ（ｘ，ｙ）において、素体上の楕円曲線の標準形$By^2=x^3+Ax^2+Bx$の場合、モンゴメリのスカラー倍を用いる。（ｂ）スカラー倍ｄ（ｘ，ｙ）を計算する場合、このアフィン座標（ｘ，ｙ）

を射影座標する際に、乱数ｋを生成し、（ｘ，ｙ）→［ｋｘ，ｋｙ，ｋ］または（ｘ，ｙ）→［k^2ｘ，k^3ｙ，ｋ］に変換する。このことにより、素体の演算対象が乱数によって常に変更する方法を用いる。

【００２１】

【発明の実施の形態】

２の拡大体上の楕円曲線の標準形$y^2+xy=x^3+ax^2+b$（ｂ≠０）のアフィン座標における演算規則を以下に示す。

【００２２】

１）０＋０＝０

２）（ｘ，ｙ）＋０＝（ｘ，ｙ）

３）（ｘ，ｙ）＋（ｘ，ｘ＋ｙ）＝０

４）可換性（ｘ０，ｙ０）＋（ｘ１，ｙ１）＝（ｘ１，ｙ１）＋（ｘ０，ｙ０）

５）加算演算（ｘ２，ｙ２）＝（ｘ１，ｙ１）＋（ｘ０，ｙ０）

$x2=a+\lambda^2+\lambda+x0+x1$；$y2=\lambda(x1+x2)+x2+y1$；

$\lambda=(y0+y1)/(x0+x1)$

６）２倍演算（ｘ２，ｙ２）＝（ｘ１，ｙ１）＋（ｘ１，ｙ１）＝２（ｘ１，ｙ１）

$x2=a+\lambda^2+\lambda$；$y2=\lambda(x1+x2)+x2+y1$；$\lambda=x1+(y1/x1)$

または、$x2=(x1)^2+b/(x1)^2$

かかる楕円曲線は、その計算を容易にするためにアフィン座標における楕円曲線上の点（Ｘ，Ｙ）を射影座標で表現することもある。任意の$\lambda\neq0$について，［Ｘ，Ｙ，Ｚ］＝［λ^2Ｘ，λ^3Ｙ，λＺ］となる射影座標を考えると、アフィン座標とこの射影座標の対応は以下で与えられる。すなわち、アフィン座標（ｘ，ｙ）は、射影座標［ｘ，ｙ，１］で表現され、射影座標［Ｘ，Ｙ，Ｚ］は、アフィン座標（$X/(Z)^2$，$Y/(Z)^3$）となる。また、射影座標において－［Ｘ，Ｙ，Ｚ］＝［Ｘ，ＸＺ＋Ｙ，Ｚ］である。

【００２３】

以下、本発明の実施例を図面を用いて具体的に説明する。図１０は、楕円曲線暗号システムの構成図である。入出力インターフェース１００１は暗号化する平文を入力するキーボード等の入力装置、復号化した平文を出力するディスプレー、プリンタ等の出力装置、平文を記憶するメモリ等の記憶装置などである。暗号化部１００２は、楕円曲線生成部１００３で生成された楕円曲線と、公開鍵、暗号鍵生成部１００４からの鍵とを入力し、平文を暗号化する。ここで、公開鍵、暗号鍵は対になっており、どちらの鍵を暗号化部１００２、復号化部１００６に与えるかは暗号システムの用途、即ち、秘密通信に用いるか、署名・認証と呼ばれる通信に用いるか等で使い分ける。暗号化された暗号文は接続インターフェース１００５から送信される。復号化部１００６は、暗号文を復号化し平文にする。

【００２４】

図１は、楕円曲線暗号システムにおける処理の流れを示す図である。楕円曲線生成部１０１では楕円曲線暗号に使用する楕円曲線を生成する。公開鍵／秘密鍵生成部１０２では、楕円曲線生成部１０１で生成した楕円曲線を入力し、これに基づいて公開鍵１１５と秘密鍵１１６を生成する。暗号化部１０３では、平文１１３、公開鍵１１５、楕円曲線を入力して暗号文１１２を出力する。復号化部１０４では、暗号文１１２、秘密鍵１１６、楕円曲線を入力し、平文１１４を出力するが、ここで出力する平文１１４は平文１１３と内容が同じものである。

【００２５】

楕円曲線生成部１０１では以下の手順で楕円曲線を生成する。原始多項式(primitive polynomials)設定１０５では、素体F_2上の原始多項式ｆ（ｘ）を設定する。例えば、素体F_2上の原始多項式は、A.Menezes, P.Oorschot, S.Vanstone, "Handbook of Applied Cryptography", CRC Press(1996)の第4.5.3 Primitive polynomialsに記述されている。

【００２６】

楕円曲線パラメタ設定１０６は、２の拡大体Ｆｑを定義体とする楕円曲線$y^2+xy=x^3+ax^2+b$のパラメタａ，ｂを設定する。安全な楕円曲線とする

ためには、楕円曲線の位数＃Ｅ（Ｆｑ）が大きな素因数ｒを持つ必要がある。＃Ｅ（Ｆｑ）＝ｋｒの場合、ｋを小さな整数とすることによって、ｒは大きな素数となる。大きな素因数ｒを位数に持つ楕円曲線を生成する方法として、文献Henri Cohen, "A Course in Computational Algebraic Number Theory",GTM138, Springer(1993) p.464 Atkin's Testで記述されている方法がある。なお、他の楕円曲線の位数が大きな素因数ｒを持つ楕円曲線パラメタ設定法を用いても本発明の実施は可能である。

【００２７】

ベースポイント生成部１０７は、楕円曲線上のアーベル群において、上記ｒを位数とする部分巡回群の生成元を求める。例えば、＃Ｅ（Ｆｑ）＝ｋｒの場合は、第１のステップでＥ（Ｆｑ）上の任意の点（ｘ１，ｙ１）を求める。次に第２のステップでｒ（ｘ１，ｙ１）＝０かつｋ（ｘ１，ｙ１）≠０の場合、Ｇ＝（ｘ１，ｙ１）をベースポイントとする。他の場合は、第１のステップへ戻る。

【００２８】

ここで、ｒ（ｘ１，ｙ１）は、（ｘ１，ｙ１）のスカラー倍（ｒ倍）演算を実行するという意味である。スカラー倍（ｒ倍）演算については楕円曲線演算部１０９で説明する。

【００２９】

以上、楕円曲線生成部１０１により、原始多項式ｆ（ｘ）、楕円曲線$y^2+xy=x^3+ax^2+b$のパラメタａ，ｂ、ベースポイントＧ、ベースポイントの位数ｒを生成した。これらは公開する情報である。

【００３０】

次に公開鍵／秘密鍵生成部１０２は、以下の手順で公開鍵と秘密鍵を生成する。入力を原始多項式ｆ（ｘ）、楕円曲線$y^2+xy=x^3+ax^2+b$のパラメタａ，ｂ、ベースポイントＧとし、出力を公開鍵Ｑ、秘密鍵ｄとすると、第１のステップで乱数２＜ｄ＜ｒ－１を生成し、第２のステップでＱ＝　ｄＧすなわちＧのスカラ倍（ｄ倍）点を求める。

【００３１】

公開鍵は、公開する情報であり、秘密鍵は秘密にする情報である。Ｑ，Ｇから

ｄを求める問題は、離散対数問題といわれるものであり、楕円曲線において、ベースポイントの位数ｒのビット長の指数オーダの計算量を必要とする。このため、ｒが大きな素数であれば例えば、ｒ＞２の１５９乗をとれば、事実上、Ｑ，Ｇからｄを求めることはできなくなる。これが楕円曲線暗号の原理である。なお、Ｑを計算する方法は、従来技術文献　D.V.Chudnovsky, G.V.Chudnovsky "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, 7, 385-434,1986で記載されている方法で求めることができる。

【００３２】

次に、暗号化部１０３では、以下の手順で平文１１３を暗号文１１４に変換する。入力を平文Ｍ、公開鍵Ｑ、原始多項式ｆ（ｘ）、楕円曲線$y^2+xy=x^3+ax^2+b$のパラメタｂ、ベースポイントＧとし、出力を暗号文Ｃとすると、第１のステップで乱数ｋを生成し（乱数生成部１０８）、第２のステップでベースポイントＧと第１のステップで生成した乱数ｋとを演算し、ｋＧすなわち（ｋｘ１，ｋｙ１）とする（楕円曲線演算部１０９）。第３のステップで公開鍵Ｑと第１のステップで生成した乱数ｋとを演算し、ｋＱすなわち（ｋｘ２，ｋｙ２）とする（楕円曲線演算部１０９）。第４のステップでＭ　ｘｏｒ　ｘ２を演算し、Ｍ'とする（データ暗号化１１０）。第５のステップでｘ１||ｙ１||Ｍ'を演算し暗号文Ｃとする（データ暗号化１１０）。

【００３３】

楕円曲線演算部１０９は、任意の点Ｒのスカラ倍ｋＲ演算を行いそのｘ座標を得る。これにより２の拡大体上の楕円曲線暗号の復号化処理時間において、処理時間の偏差情報から秘密鍵情報が漏れなくなる。以下にこのスカラー倍方法を説明する。図２、図３は、このスカラー倍方法の第１の実施例の説明図である。

【００３４】

＜第１実施例スカラー倍方法＞

Ｒのｘ座標の射影座標成分X_0、スカラー値ｍを入力とし、Ｒのｍ倍の点のｘ座標の射影座標成分X_mを出力とする。ｍ，X_0を入力を入力し（ステップ２０２）、ステップ２０３から２０５では乱数を射影座標の各座標に乗算することに

より、データを撹拌する。すなわち、乱数ｋを生成し（ステップ２０３）、乱数ｋとX_0を演算してk^2X_0をX_1に代入し、乱数ｋをZ_1に代入する（ステップ２０５）。ステップ２０６から２０８及び３０１ではスカラー倍の準備を行う。すなわち、$[X_1, Z_1]$を$[X_4, Z_4]$に代入し（ステップ２０６）、また$[X_1, Z_1]$を２倍方法（図５）に入力し、出力を$[X_2, Z_2]$へ代入する（ステップ２０７）。　ｍの２進数表現を$h_i h_{i-1} \cdots h_0$とする（ステップ２０８）。ただし、最上位ビットh_1は１である。ｉを１とする（ステップ３０１）。ステップ３０２から３０９ではｍの１ビットが０か１かによって加算方法や２倍方法を制御しスカラー倍を求める。すなわち、　ｉ－１をｉに代入し（ステップ３０２）、$[X_1, Z_1]$、$[X_2, Z_2]$、$[X_4, Z_4]$を加算方法（図４）に入力し、出力を$[X_3, Z_3]$へ代入する（ステップ３０３）。ここで、h_i＝＝０ならば、ステップ３０４へ、１ならばステップ３０６へ進む（ステップ３０４）。$[X_1, Z_1]$を２倍方法（図５）に入力し、出力を$[X_1, Z_1]$に代入する（ステップ３０５）。$[X_3, Z_3]$を$[X_2, Z_2]$に代入し、ステップ３０８へいく（ステップ３０６）。$[X_2, Z_2]$を２倍方法（図５）に入力し、出力を$[X_2, Z_2]$に代入する（ステップ３０７）。$[X_3, Z_3]$を$[X_1, Z_1]$に代入し、ステップ３０８へいく（ステップ３０８）。ｉ＞０ならばステップ３０２へ進む（ステップ３０９）。次は、射影座標から（ｘ，ｙ）座標のｘ座標へ変換する。$X_1/(Z_1)^2$をX_mに代入し（ステップ３１０）、X_mを出力する（ステップ３１１）。

【００３５】

次に、加算方法について説明する。楕円曲線上の点の射影空間座標として、任意の$\lambda \neq 0$について，$[X, Y, Z] = [\lambda^2 X, \lambda^3 Y, \lambda Z]$とする。ここで、楕円曲線上の点Ｐ０＝（ｘ０，ｙ０）＝$[X_0, Y_0, Z_0]$；Ｐ１＝（ｘ１，ｙ１）＝$[X_1, Y_1, Z_1]$とする。この和と差をＰ３＝（ｘ３，ｙ３）＝$[X_3, Y_3, Z_3]$，Ｐ４＝（ｘ４，ｙ４）＝$[X_4, Y_4, Z_4]$とする。

【００３６】

Ｐ１＋Ｐ０＝Ｐ３；

Ｐ１－Ｐ０＝Ｐ４；

$x3=a+(\lambda_3)^2+\lambda_3+x0+x1$；$\lambda_3=(y0+y1)/(x0+x1)$；

$x4=a+(\lambda_4)^2+\lambda_4+x0+x1$；$\lambda_4=(x0+y0+y1)/(x0+x1)$；

$\lambda_3+\lambda_4=(x0)/(x0+x1)$；

$(\lambda_3)^2+(\lambda_4)^2=(x0)^2/(x0+x1)^2$；

$x3+x4=((x0)^2+(x0)(x0+x1))/(x0+x1)^2=(x0x1)/(x0+x1)^2$；

以上により、$x3+x4=(x0x1)/(x0+x1)^2$ ―――― (1)

という関係式が得られた。

【００３７】

次に、射影座標での関係式を導出する。

【００３８】

$x1=X_1/(Z_1)^2$、$x0=X_0/(Z_0)^2$を（１）式に代入する。

$X_3/(Z_3)^2=X_4/(Z_4)^2+((X_0/(Z_0)^2)(X_1/(Z_1)^2))/(X_0/(Z_0)^2+X_1/(Z_1)^2)^2$；

$=X_4/(Z_4)^2+((X_0(Z_0)^2)(X_1(Z_1)^2))/(X_0(Z_1)^2+X_1(Z_0)^2)^2$；

$=((X_4\beta^2)+Z_4^2(X_0Z_0^2)(X_1Z_1^2))/(Z_4^2\beta^2)$

ただし、$\beta=X_0Z_1^2+X_1Z_0^2$

これより、

$X_3=X_4\beta^2+Z_4^2(X_0Z_1^2)(X_1Z_0^2)$；―――― (2)

$Z_3=Z_4\beta$；―――――――――――――――――― (3) を得た。

【００３９】

ここで、$mR=[X_1, Y_1, Z_1]$、$(m+1)R=[X_2, Y_2, Z_2]$、$R=[X_4, Y_4, Z_4]$、$(2m+1)R=[X_3, Y_3, Z_3]$とする。この導出式を利用した加算方法を以下に説明する。図４はこの方法の説明図であ

る。

【００４０】

＜第１実施例加算方法＞

射影座標［X_1，Z_1］，［X_2，Z_2］，［X_4，Z_4］を入力とし、［X_3，Z_3］または無限遠点を出力とする。［X_1Z_1］，［X_2，Z_2］，［X_4，Z_4］を入力し（ステップ４０２）、ステップ４０３から４０７では加算結果が無限遠点か判定するために$X_1(Z_2)^2+X_2(Z_1)^2$を求める。さらに各中間結果S_1、S_2、Ｂは、上記式（２），（３）を求めるための準備である。すなわち、$X_1(Z_2)^2$をS_1に代入し（ステップ４０３）、$X_2(Z_1)^2$をS_2に代入し（ステップ４０４）、S_1+S_2をＢに代入し（ステップ４０５）、Ｂ＝０の場合、ステップ４０７へ進み、成立しない場合ステップ４０８へ進む（ステップ４０６）。ステップ４０７では、無限遠点を出力し、ステップ４１３へいく。以下の４０８－４１１は上記式（２），（３）に従って［X_3，Z_3］を求める。Z_4ＢをZ_3に代入し（ステップ４０８）、$(Z_4)^2S_1S_2$をＳに代入し（ステップ４０９）、$X_4Z_3^2$をＭに代入し（ステップ４１０）、　Ｍ＋ＳをX_3に代入し（ステップ４１１）、［X_3，Z_3］を出力を出力する（ステップ４１２）。かかる方法により相異なる変数の乗算６回で加算演算を実行できる。すなわち、X_1、X_2、X_4からX_3を高速に演算できる。

【００４１】

次に、２倍計算方法について説明する。Ｐ１の２倍点をＰ２とし、Ｐ１＝（ｘ１，ｙ１）＝［X_1，Y_1，Z_1］、Ｐ２＝（ｘ２，ｙ２）＝［X_2，Y_2，Z_2］とする。２倍演算の演算式　$x2=(x1)^2+b/(x1)^2$より、ｘ１＝　$X_1/(Z_1)^2$、ｘ２＝$X_2/(Z_2)^2$をこの式に代入する。

【００４２】

$X_2/(Z_2)^2=(X_1/(Z_1)^2)^2+b/(X_1/(Z_1)^2)^2=X_1^2/(Z_1)^4+(b(Z_1)^4)/(X_1)^2=(X_1^4+b(Z_1)^8)/(X_1^2Z_1^4)$

従って、

$X_2=X_1^4+bZ_1^8$－－－－－（４）

$Z_2=X_1Z_1^2$－－－－－－－－－（５）

この導出式を利用した２倍方法を以下に説明する。図５は、この説明図である。

【００４３】

＜第１実施例２倍計算方法＞

Ｑ＝［X_1，Z_1］、ｂを入力とし、２Ｑ＝［X_2，Z_2］または無限遠点を出力とする。X_1，Z_1を入力し（ステップ５０２）、以下のステップ５０３から５０４は２倍結果が無限遠点を判定するためにX_1＝＝０またはZ_1＝＝０の判定を行う。すなわち、X_1＝＝０またはZ_1＝＝０の場合は、ステップ５０４へ。成立しない場合は、ステップ５０５へいく（ステップ５０３）。ステップ５０４では、無限遠点を出力する。以下のステップ５０５から５０７では上記式（４），（５）に従って［X_2，Z_2］を求める。Z_1^2をＳに代入し（ステップ５０５）、　X_1ＳをＺ$_2$に代入し（ステップ５０６）、X_1^4＋ｂ（Ｓ）^{4}をX_2に代入し（ステップ５０７）、［X_2，Z_2］を出力する（ステップ５０８）。かかる方法により相異なる変数の乗算２回で加算演算を実行できる。従って、＜スカラー倍方法＞においてはスカラー値ｄのビットあたり、相異なる変数の乗算６＋２＝８回で実行できる。すなわち、X_1、X_2、X_4からX_3を高速に演算できる。

【００４４】

つぎに、復号化部１０４では、以下の手順で暗号文１１２を元の平文１１４に変換する。１１２と１１４は内容が同じ平文である。入力を暗号文Ｃ←ｘ１||ｙ１||Ｍ’、秘密鍵ｄ、原始多項式ｆ（ｘ）、楕円曲線$y^2+xy=x^3+ax^2$＋ｂのパラメタ，ｂ、ベースポイントＧとし、出力を平文Ｍとする。

【００４５】

ステップ１：（ｘ２，ｙ２）←ｄ（ｘ１，　ｙ１）（楕円曲線演算部１１１）

ステップ２：平文Ｍ←Ｍ’　ｘｏｒ　ｘ２

ステップ１は図２、図３を用いて実行する。

【００４６】

以上により、与えられた座標（ｘ，ｙ）のｄスカラー倍のｘ座標を求める処理

において、　ｄのビットパターンに依存せず、ｄの各ビットあたり８回の相異なる乗算処理で実現することができる。また、ｄの与えられたｘ座標に対して、乱数ｋにより［ｋｘ^2，ｋ］をスカラー倍初期値とすることによって、常に演算対象を変動させることができる。さらに、これらの組合わせにより、ｄのビットパターンが、ｄ（ｘ，ｙ）処理時間の偏差に現れないため、ｄ（ｘ，ｙ）処理時間の偏差情報から秘密鍵情報がもれない方法を示した。また、この性質は暗号処理の電流、電圧、電力の偏差を用いて、暗号解読を行うＤＰＡ(Differential Power Analysis)に対して、ｄ（ｘ，ｙ）の処理電流（電圧、電力）の偏差情報から秘密鍵情報がもれない方法をも示している。

【００４７】

次に第１実施例を更に高速化を図ることが可能な第２実施例を説明する。アフィン座標から、射影座標への変換を（ｘ，ｙ）→［ｘ，ｙ，１］とする場合、$Z_4=1$とできる。（２）、（３）式に$Z_4=1$を代入すると、

$$X_3=(X_4\beta^2)+(X_0(Z_1)^2)(X_0(Z_1)^2) \quad \text{----------（６）}$$

$$Z_3=\beta \quad \text{----------（７）}$$

この式を利用してスカラー倍方法、加算方法を以下のように求めることができる。

【００４８】

＜第２実施例スカラー倍方法＞

これを図６、図７に示す。Ｒのｘ座標の射影座標成分X_0、スカラー値ｍを入力とし、　Ｒのｍ倍の点のｘ座標の射影座標成分X_mを出力とする。ｍ，X_0を入力し（ステップ６０２）、以下のステップ６０３から６０４ではX_0を射影座標に変換する。X_0をX_1に代入し（ステップ６０３）、１をZ_1に代入する（ステップ６０４）。ステップ６０５から６０７ではスカラー倍の準備を行う。すなわち、［X_1，Z_1］を［X_4，Z_4］に代入し（ステップ６０５）、［X_1，Z_1］を２倍方法（図５）に入力し、出力を［X_2，Z_2］へ代入する（ステップ６０６）。ｍの２進数表現を$h_i h_{i-1} \cdots h_0$とする（ステップ６０７）。ただし、最上位ビットh_iは１である。１をｉに代入する（ステップ７０１）。以下のステップ７０２から７０９ではｍの１ビットが０か１かによって加

算方法や２倍方法を制御しスカラー倍を求める。すなわち、ｉ－１をｉに代入し（ステップ７０２）、$[X_1, Z_1]$、$[X_2, Z_2]$、X_0を加算方法（図８）に入力し、出力を$[X_3, Z_3]$へ代入する（ステップ７０３）。$h_i == 0$ならば、ステップ７０６へ、１ならばステップ７０８へ進む（ステップ７０４）。$[X_1, Z_1]$　を２倍方法（図５）に入力し、出力を$[X_1, Z_1]$に代入する（ステップ７０５）。$[X_3, Z_3]$を$[X_2, Z_2]$に代入し、ステップ７１０へいく（ステップ７０６）。$[X_2, Z_2]$を２倍方法（図５）に入力し、出力を$[X_2, Z_2]$に代入する（ステップ７０７）。$[X_3, Z_3]$を$[X_1, Z_1]$へ代入し、ステップ７１０へいく（ステップ７０８）。ｉ＞０ならばステップ７０３へ進む（ステップ７０９）。$X_1 / (Z_1)^2$をX_mに代入し（ステップ７１０）、X_mを出力する（ステップ７１１）。

【００４９】

＜第２実施例加算方法＞

これを図８に示す。$[X_1, Z_1]$，$[X_2, Z_2]$，X_4を入力とし、$[X_3, Z_3]$または無限遠点を出力とする。$[X_1, Z_1]$，$[X_2, Z_2]$，X_4を入力し（ステップ８０２）、以下のステップ８０３から８０７は加算結果が無限遠点か判定するために$X_1 (Z_2)^2 + X_2 (Z_1)^2$を求める。さらに各中間結果$S_1$、$S_2$、Ｂは、上記式（６），（７）を求めるための準備である。すなわち、$X_1 Z_2^2$をS_1に代入し（ステップ８０３）、$X_2 Z_1^2$をS_2に代入し（ステップ８０４）、$S_1 + S_2$をＢに代入する（ステップ８０５）。Ｂ＝＝０の場合は、ステップ８０７へ進み、成立しない場合ステップ８０８へ進む（ステップ８０６）。無限遠点を出力し、ステップ８１３へいく（ステップ８０７）。以下のステップ８０８から８１１は上記式（６），（７）に従って$[X_3, Z_3]$を求める。すなわち、ＢをZ_3に代入し（ステップ８０８）、S_1 S_2をＳに代入し（ステップ８０９）、$X_4 Z_3^2$をＭに代入し（ステップ８１０）、Ｍ＋ＳをX_3に代入し（ステップ８１１）、$[X_3, Z_3]$を出力する（ステップ８１２）。

【００５０】

以上により、相異なる変数の乗算４回で加算演算を実行できる。このため、第

１実施例の加算演算より、乗算回数を減らすことができる。なお、２倍演算は第１実施例の２倍演算を利用する。

【００５１】

上述した処理時間の偏差情報から秘密鍵情報が漏れない方法は、２の拡大体上の楕円曲線の場合の他、素体上の楕円曲線でも適用可能である。

【００５２】

次に第３実施例を説明する。素体上の楕円曲線$By^2=x^3+Ax^2+Bx$の場合、モンゴメリ法を用いて、処理時間の偏差情報から秘密鍵情報がもれない方法を示す。

【００５３】

P.Montgomery,"Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation Vol.48,No.177,pp.243-264(1987)では、有限素体上の楕円曲線の標準形　$By^2=x^3+Ax^2+Bx$を用いて、点Ｐ０（ｘ０，ｙ０），Ｐ１（ｘ１，ｙ１）の加算と、減算を

Ｐ３（ｘ３，ｙ３）；　Ｐ４（ｘ４，ｙ４）；

Ｐ１＋Ｐ０＝Ｐ３　　；

Ｐ１－Ｐ０＝Ｐ４　　；　とするとき、

ｘ０，ｘ１，ｘ４から、ｘ３が高速に求まる。具体的には、次のように素体の乗算６回で求まる。

【００５４】

$(x_3, y_3) \rightarrow [X_3, Z_3]$；$(x_4, y_4) \rightarrow [X_4, Z_4]$；

とするとき、

$X_3 \leftarrow Z_4 [(X_1-Z_1)(X_0+Z_0)+(X_1+Z_1)(X_0-Z_0)]^2$　；

$Z_3 \leftarrow X_4 [(X_1-Z_1)(X_0+Z_0)-(X_1+Z_1)(X_0-Z_0)]^2$　；

また、２倍演算は、

$P5=2P1$；$(x_1, y_1) \rightarrow [X_1, Z_1]$；

$4X_1Z_1 \leftarrow (X_1+Z_1)^2-(X_1-Z_1)^2$　；

$X_5 \leftarrow (X_1+Z_1)^2(X_1-Z_1)^2$; $Z_5 \leftarrow (4X_1Z_1)[(X_1-Z_1)^2+((A+2)/4)(4X_1Z_1)]$ ；

また、Ｐ１の２倍点Ｐ５（ｘ５，ｙ５）とするとき、ｘ５は、ｘ１のみから求まり、乗算５回である。これを利用して、点Ｒのスカラ倍（スカラー値ｄ）のｘ座標を以下のようにＲｘから求める。

【００５５】

初期値を［Ｒ，２Ｒ］、ｍＲをＲのｍ倍のｘ座標とするとき、ｄを２進数展開し、ｄの上位ビットから、

０の場合、［ｍＲ，（ｍ＋１）Ｒ］→［２ｍＲ，（２ｍ＋１）Ｒ］

１の場合、［ｍＲ，（ｍ＋１）Ｒ］→［（２ｍ＋１）Ｒ，２（ｍ＋１）Ｒ］

（ｍ＋１）Ｒ－ｍＲ＝Ｒ

（ｍ＋１）Ｒ＋ｍＲ＝（２ｍ＋１）Ｒである。

【００５６】

＜第３実施例スカラー倍方法＞

Ｒのｘ座標の射影座標成分X_0、スカラー値ｍを入力とし、Ｒのｍ倍の点のｘ座標の射影座標成分X_mを出力とする。　ｍ，X_0を入力を入力し（ステップ９０２）、ステップ９０３から９０５では乱数を射影座標の各座標に乗算することにより、データを撹拌する。すなわち、乱数ｋを生成し（ステップ９０３）、乱数ｋとX_0を演算してkX_0をX_1に代入し（ステップ９０４）、乱数ｋをZ_1に代入する（ステップ９０５）。次に、［X_1，Z_1］を［X_4，Z_4］に代入し（ステップ９０６）、［X_1，Z_1］を２倍方法（モンゴメリの２倍演算）に入力し、出力を［X_2，Z_2］へ代入する（ステップ９０７）。ｍの２進数表現を$h_i h_{i-1} \cdots h_0$とする（ステップ９０８）。ただし、最上位ビットh_1は１である。ｉを１とする（ステップ９０９）。ｉ－１をｉに代入し（ステップ９１０）、［X_1，Z_1］、［X_2，Z_2］、［X_4，　Z_4］を加算方法（モンゴメリの加算演算）に入力し、出力を［X_3，Z_3］へ代入する（ステップ９１１）。ここで、h_i＝＝０ならば、ステップ９１２へ、１ならばステップ９１４へ進む（ステップ９１２）。［X_1，Z_1］を２倍方法（モンゴメリの２倍演算）に入力し、出力を［X_1，Z_1］に代入する（ステップ９１３）。［X_3，Z_3］を［X_2，Z_2］に代入し、ステップ９１６へいく（ステップ９１４）

。［X_2，Z_2］を２倍方法（モンゴメリの２倍演算）に入力し、出力を［X_2，Z_2］に代入する（ステップ９１５）。［X_3，　Z_3］を［X_1，Z_1］に代入し、ステップ９１６へいく（ステップ９１６）。ｉ＞０ならばステップ９１０へ進む（ステップ９１７）。X_1/Z_1をX_mに代入し（ステップ９１８）、X_mを出力する（ステップ９１９）。

【００５７】

以上により、与えられた座標（ｘ，ｙ）のｄスカラー倍のｘ座標を求める処理において、ｄの各ビットあたり１１回の相異なる乗算処理で実現し、与えられたｘ座標に対して、乱数ｋにより［ｋｘ，ｋ］をスカラー倍初期値とすることによって、ｄ（ｘ，ｙ）処理時間の偏差情報から秘密鍵情報がもれない方法を示した。また、この性質は暗号処理の電流、電圧、電力の偏差を用いて、暗号解読を行うＤＰＡに対して、ｄ（ｘ，ｙ）の処理電流（電圧、電力）の偏差情報から秘密鍵情報がもれない方法を示している。

【００５８】

さらに、素体上の楕円曲線$y^2=x^3+ax+b$の場合、$By^2=x^3+Ax^2+Bx$と$y^2=x^3+ax+b$の間に有理点がなすアーベル群が同型となる楕円曲線を構成し、素体上の楕円曲線$y^2=x^3+ax+b$で与えられた（ｘ，ｙ）を$By^2=x^3+Ax^2+Bx$に変換し、上記発明の方法でスカラー倍を求め、結果を$y^2=x^3+ax+b$に変換することにより本発明を利用することができる。

【００５９】

次に第４実施例を説明する。第１実施例では、射影座標を任意の$\lambda\neq0$について，［Ｘ，Ｙ，Ｚ］＝［λ^2X，λ^3Y，λZ］とするものを説明したが、［Ｘ，Ｙ，Ｚ］＝［λX，λY，λZ］とする射影座標で実施することもできる。

【００６０】

＜第４実施例スカラー倍方法＞

Ｒのｘ座標の射影座標成分X_0、スカラー値ｍを入力とし、Ｒのｍ倍の点のｘ座標の射影座標成分X_mを出力とする。ｍ，X_0を入力し（ステップ１００２）、以下のステップ１００３から１００５では乱数を射影座標の各座標に乗算する

ことにより、データを撹拌する。すなわち、乱数ｋを生成し（ステップ１００３）、ｋX_0をX_1に代入し（ステップ１００４）、乱数ｋをZ_1に代入する（ステップ１００５）。［X_1，Z_1］を［X_4，Z_4］に代入し（ステップ１００６）、［X_1，Z_1］を２倍方法に入力し、出力を［X_2，Z_2］へ代入する（ステップ１００７）。ｍの２進数表現を$h_i h_{i-1} \cdots h_0$とする（ステップ１００８）。ただし、最上位ビットh_1は１である。ｉを１とする（ステップ１００９）。ｉ－１をｉに代入し（ステップ１０１０）、［X_1，Z_1］、［X_2，Z_2］、［X_4，Z_4］を加算方法に入力し、出力を［X_3，Z_3］へ代入する（ステップ１０１１）。ここで、h_i＝＝０ならば、ステップ１０１２へ、１ならばステップ１０１４へ進む（ステップ１０１２）。［X_1，Z_1］を２倍方法に入力し、出力を［X_1，Z_1］に代入する（ステップ１０１３）。［X_3，Z_3］を［X_2，Z_2］に代入し、ステップ１０１６へいく（ステップ１０１４）。［X_2，Z_2］を２倍方法に入力し、出力を［X_2，Z_2］に代入する（ステップ１０１５）。［X_3，Z_3］を［X_1，　Z_1］に代入し、ステップ１０１６へいく（ステップ１０１６）。ｉ＞０ならばステップ１０１０へ進む（ステップ１０１７）。X_1／Z_1をX_mに代入し（ステップ１０１８）、X_mを出力する（ステップ１０１９）。

【００６１】

楕円曲線上の点の射影空間座標として、任意のλ≠０について，［Ｘ，Ｙ，Ｚ］＝［λＸ，　λＹ，λＺ］とする。ここで、楕円曲線上の点Ｐ０＝（ｘ０，ｙ０）＝［X_0，Y_0，Z_0］；　Ｐ１＝（ｘ１，ｙ１）＝［X_1，Y_1，Z_1］とする。この和と差をＰ３＝（ｘ３，ｙ３）＝［X_3，Y_3，Z_3］，Ｐ４＝（ｘ４，ｙ４）＝［X_4，Y_4，Z_4］とする。

【００６２】

Ｐ１＋Ｐ０＝Ｐ３；

Ｐ１－Ｐ０＝Ｐ４；

第１実施例の（１）式ｘ３＋ｘ４＝（ｘ０ｘ１）／（ｘ０＋ｘ１）^{2}より射影座標での関係式を導出する。

【００６３】

$x1=X_1/Z_1$、$x0=X_0/Z_0$を（１）式に代入する。

$X_3/Z_3=X_4/Z_4+((X_0/Z_0)(X_1/Z_1))/(X_0/Z_0+X_1/Z_1)^2$；

$=X_4/(Z_4)^2+((X_0Z_0)(X_1Z_1))/(X_0Z_1+X_1Z_0)^2$；

$=((X_4\beta^2)+Z_4^2(X_0Z_0)(X_1Z_1))/(Z_4^2\beta^2)$

ただし、$\beta=X_0Z_1+X_1Z_0$

これより、$X_3=(X_4\beta^2)+Z_4^2(X_0Z_1)(X_1Z_0)$；－－（２）’

$Z_3=Z_4^2\beta^2$；－－－－－－－－－－－－－－－－－－－－－－（３）’

を得た。

【００６４】

ここで、$mR=[X_1, Y_1, Z_1]$、$(m+1)R=[X_2, Y_2, Z_2]$、$R=[X_4, Y_4, Z_4]$、$(2m+1)R=[X_3, Y_3, Z_3]$とする。この導出式を利用した加算方法を以下に説明する。

【００６５】

＜第４実施例加算方法＞

射影座標$[X_1, Z_1]$，$[X_2, Z_2]$，$[X_4, Z_4]$を入力とし、$[X_3, Z_3]$ または無限遠点を出力とする。$[X_1, Z_1]$，$[X_2, Z_2]$，$[X_4, Z_4]$を入力し（ステップ１１０２）、X_1Z_2をS_1に代入し（ステップ１１０３）、X_2Z_1をS_2に代入し（ステップ１１０４）、S_1+S_2をＢに代入する（ステップ１１０５）。Ｂ＝＝０の場合は、ステップ１１０７へ進み、成立しない場合ステップ１１０８へ進む（ステップ１１０６）。無限遠点を出力し、ステップ１１１３へいく（ステップ１１０７）。$(Z_4)^2B^2$をZ_3に代入し（ステップ１１０８）、$(Z_4)^2S_1S_2$をＳに代入し（ステップ１１０９）、(X_4B^2)をＭに代入し（ステップ１１１０）、Ｍ＋ＳをＸ$_3$に代入し（ステップ１１１１）、$[X_3, Z_3]$を出力する（ステップ１１１

２）。

【００６６】

以上により、相異なる変数の乗算６回で加算演算を実行できる。

【００６７】

次に、２倍計算方法について説明する。Ｐ１の２倍点をＰ２とし、Ｐ１＝（ｘ１，ｙ１）＝［X_1，Y_1，Z_1］、Ｐ２＝（ｘ２，ｙ２）＝［X_2，Y_2，Z_2］とする。２倍演算の演算式　$x2=(x1)^2+b/(x1)^2$より、$x1=X_1/Z_1$、$x2=X_2/Z_2$をこの式に代入する。

【００６８】

$$X_2/Z_2=(X_1/Z_1)^2+b/(X_1/Z_1)^2=X_1^2/(Z_1)^2+(bZ_1^2)/(X_1)^2=(X_1^4+bZ_1^4)/(X_1^2Z_1^2)$$

従って、

$$X_2=X_1^4+bZ_1^4 \quad \text{------（４）'}$$

$$Z_2=X_1^2Z_1^2 \quad \text{----------（５）'}$$

この導出式を利用した２倍方法を以下に説明する。

【００６９】

＜第４実施例２倍計算方法＞

Ｑ＝［X_1，Z_1］，ｂを入力とし、２Ｑ＝［X_2，Z_2］または無限遠点を出力する。X_1，Z_1を入力し（ステップ１２０２）、X_2＝＝０またはZ_2＝＝０の場合、ステップ１２０４へ。成立しない場合、ステップ１２０５へいく（ステップ１２０３）。ステップ１２０４では、無限遠点を出力する。$Z_2=X_1^2Z_1^2$とし（ステップ１２０５）、$S=bZ_1^4$とし（ステップ１２０６）、X_1^4+SをX_2に代入し（ステップ１２０７）、［X_2，Z_2］を出力する（ステップ１２０８）。かかる方法により、相異なる変数の乗算２回で加算演算を実行できる。

【００７０】

以上により、与えられた座標（ｘ，ｙ）のｄスカラー倍のｘ座標を求める処理において、ｄの各ビットあたり８回の相異なる乗算処理で実現し、与えられたｘ座標に対して、乱数ｋにより［ｋｘ，ｋ］をスカラー倍初期値とすることによって、ｄ（ｘ，ｙ）処理時間の偏差情報から秘密鍵情報がもれない方法を示した。

暗号解読ＤＰＡに対して、ｄ（ｘ，ｙ）の処理電流（電圧、電力）の偏差情報から秘密鍵情報がもれない方法を示している。

【００７１】

次に第５実施例を説明する。第２実施例では、射影座標を任意のλ≠０について，［Ｘ，Ｙ，Ｚ］＝［λ^2Ｘ，λ^3Ｙ，λＺ］とするものを説明したが、［Ｘ，Ｙ，Ｚ］＝［λＸ，λＹ，λＺ］とする射影座標で実施することもできる。

【００７２】

アフィン座標から、射影座標への変換を（ｘ，ｙ）→［ｘ，ｙ，１］とする場合、Z_4＝１　とできる。

【００７３】

＜第５実施例スカラー倍方法＞

Ｒのｘ座標の射影座標成分X_0、スカラー値ｍを入力とし、Ｒのｍ倍の点のｘ座標の射影座標成分X_mを出力とする。ｍ，X_0を入力し（ステップ１３０２）、乱数ｋを生成し（ステップ１３０３）、ｋX_0をX_1に代入する（ステップ１３０４）。１をZ_1に代入する（ステップ１３０５）。［X_1，Z_1］を［X_4，Z_4］に代入し（ステップ１３０６）、［X_1，Z_1］を２倍方法に入力し、出力を［X_2，Z_2］へ代入する（ステップ１３０７）。ｍの２進数表現をh_i h_{i-1}・・・h_0とする。ただし、最上位ビットh_iは１である（ステップ１３０８）。１をｉに代入する（ステップ１３０９）。ｉ－１をｉに代入し（ステップ１３１０）、［X_1，　Z_1］、［X_2，Z_2］、X_4を加算方法に入力し、出力を［X_3，Z_3］へ代入する（ステップ１３１１）。h_i＝＝０ならば、ステップ１３１２へ、１ならばステップ１３１４へ進む（ステップ１３１２）。［X_1，Z_1］を２倍方法に入力し、出力を［X_1，Z_1］に代入する（ステップ１３１３）。［X_3，Z_3］を［X_2，Z_2］へ代入し、ステップ１３１６へいく（ステップ１３１４）。［X_2，Z_2］を２倍方法に入力し、出力を［X_2，Z_2］に代入する（ステップ１３１５）。［X_3，Z_3］を［X_1，Z_1］へ代入し、ステップ１３１６へいく（ステップ１３１６）。ｉ＞０ならばステップ１３００へ進む（ステップ１３１７）。X_1／Z_1をX_mに代入し（ステップ１３１８）、X_mを出力する（ステップ１３１９）。

【００７４】

＜第５実施例加算方法＞

$[X_1, Z_1]$，$[X_2, Z_2]$，X_4を入力とし、$[X_3, Z_3]$または無限遠点を出力とする。$[X_1, Z_1]$，$[X_2, Z_2]$，X_4を入力する（ステップ１４０２）。X_1Z_2をS_1に代入し（ステップ１４０３）、X_2Z_1をS_2に代入し（ステップ１４０４）、S_1+S_2をＢに代入する（ステップ１４０５）。Ｂ＝＝０の場合、ステップ１４０７へ、成立しない場合ステップ１４０８へ進む（ステップ１４０６）。無限遠点を出力し、ステップ１４１３へいく（ステップ１４０７）。次に、B^2をZ_3に代入し（ステップ１４０８）、S_1S_2をＳに代入し（ステップ１４０９）、（X_4B^2）をＭに代入し（ステップ１４１０）、Ｍ＋ＳをX_3に代入し（ステップ１４１１）し、$[X_3, Z_3]$を出力する（ステップ１４１２）。以上により、相異なる変数の乗算４回で加算演算を実行できる。なお、２倍演算は、前述した実施例の２倍演算を利用する。尚、本実施例は２の拡大体上、素体上の楕円曲線どちらにも適用可能である。

【００７５】

次に第６実施例を説明する。図１の楕円曲線演算部を、図９における９０１の楕円曲線演算装置で実施する。９０１は点のｘ座標X_0、スカラー値ｍ、２の拡大体上の楕円曲線の標準形$y^2+xy=x^3+ax^2+b$におけるｂを入力し（９０２）、ｍ倍の点のｘ座標をX_m出力する（９０３）。尚、本実施例は２の拡大体上の楕円曲線で説明するが、素体上の楕円曲線を用いた場合も同様の方法で実現可能である。

【００７６】

乱数生成部９０４は、乱数ｋを生成し、ｋを出力する（９０５）。射影座標変換部９０６には乱数生成部９０４からの乱数ｋの他、ｘ座標X_0とスカラー値ｍ、ｂを入力し（９０５）、射影座標$[kX_0, k]$に変換する。これを$[X_1, Z_1]$とする。スカラー倍部９０８は射影座標$[X_1, Z_1]$とスカラー値ｍを入力し、$[X_1, Z_1]$のｍ倍点を求め、そのｘ座標X_mを出力する。ここで、スカラー倍部９０８は、先ず、$[X_1, Z_1]$を$[X_4, Z_4]$へ代入する。かかる$[X_4, Z_4]$は、例えばスカラー倍部のメモリに予め記憶させておく。ま

た［X_1，Z_1］を９１３へ出力して、２倍点［X_2，Z_2］を得る。次に、ｍを２進数展開して、上位ビットからビットが０の場合［X_1，Z_1］を９１３に出力して９１３の出力である２倍点を［X_1，Z_1］に代入する。その後［X_1，Z_1］、［X_2，Z_2］、［X_4，Z_4］を９１０へ入力して出力である加算点を［X_2，Z_2］に代入する。ビットが１の場合［X_2，Z_2］を９１３に出力して９１３の出力である２倍点を［X_2，Z_2］に代入する。その後［X_1，Z_1］、［X_2，Z_2］、［X_4，Z_4］を９１０へ入力して出力である加算点を［X_1，Z_1］に代入することによりｍ倍の点のX_m座標を得る。

【００７７】

加算演算部９１０では、［X_1，Z_1］［X_2，Z_2］［X_4，Z_4］を入力し、［X_3，Z_3］＝［X_2，Z_2］＋［X_1，Z_1］、［X_4，Z_4］＝［X_2，Z_2］－［X_1，Z_1］となる［X_3，Z_3］を以下のように求め出力する。

【００７８】

先ず、$S_1 \leftarrow X_1 Z_2^{\,2}$、$S_2 \leftarrow X_2 Z_1^{\,2}$、$B \leftarrow S_1 + S_2$を計算する。ここでＢ＝＝０の場合、無限遠点を出力し終了となる。Ｂ＝０が成立しない場合、$Z_3 \leftarrow Z_4 B$、$S \leftarrow Z_4^{\,2} S_1 S_2$、$M \leftarrow X_4 Z_3^{\,2}$、$X_3 \leftarrow M + S$を計算する。

【００７９】

２倍演算部９１３では、［X_1，Z_1］、ｂを入力し、［X_2，Z_2］＝［X_1，Z_1］＋［X_1，Z_1］となる［X_2，Z_2］を以下のように求め出力する。すなわち、X_1＝＝０またはZ_1　＝＝０の場合、無限遠点を出力する。他の場合、$S \leftarrow Z_1^{\,2}$、$Z_2 \leftarrow X_1 S$、$X_2 \leftarrow X_1^{\,4} + b\,(S)^{\,4}$を計算する。

【００８０】

上記実施例では、ｘ座標X_0を射影座標［kX_0，ｋ］に変換した例を説明したが、射影座標［k^2X_0，ｋ］に変換する場合にも適用可能である。

【００８１】

尚、上述した実施例にかかるプログラムは記録媒体に格納しておくことも可能である。

【００８２】

【発明の効果】

本発明により前記従来のより、高速に楕円曲線暗号処理を実行できる。また、楕円曲線暗号の実行方法において、ｄ（ｘ，ｙ）の処理時間がｄのビットパターンに依存しない処理方法を与えることによって、偏差情報から秘密鍵情報がもれずに処理できる。

【図面の簡単な説明】

【図１】

本発明の楕円曲線暗号システムにおける処理の流れを示す図である。

【図２】

本発明の第１の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図３】

本発明の第１の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図４】

本発明の第１の実施例を示す楕円曲線暗号実行方法及び装置を実行するための加算演算のフローチャートである。

【図５】

本発明の第１の実施例を示す楕円曲線暗号実行方法及び装置を実行するための２倍演算のフローチャートである。

【図６】

本発明の第２の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図７】

本発明の第２の実施例を示す楕円曲線暗号実行方法及び装置においてスカラー倍方法を示すフローチャートである。

【図８】

本発明の第２の実施例を示す楕円曲線暗号実行方法及び装置を実行するための

加算演算のフローチャートである。

【図９】

本発明の楕円曲線演算装置を構成図である。

【図１０】

本発明の楕円曲線暗号システムの構成図である。

【符号の説明】

１０１　楕円曲線生成部、

１０２　公開鍵、秘密鍵生成部、

１０３　暗号化部、

１０４　復号化部、

１０５　素数生成部、

１０６　楕円曲線パラメタ設定、

１０７　ベースポイント生成部、

１０８　乱数生成部、

１０９　楕円曲線演算部、

１１０　データ暗号化処理部、

１１１　データ復号化処理部、

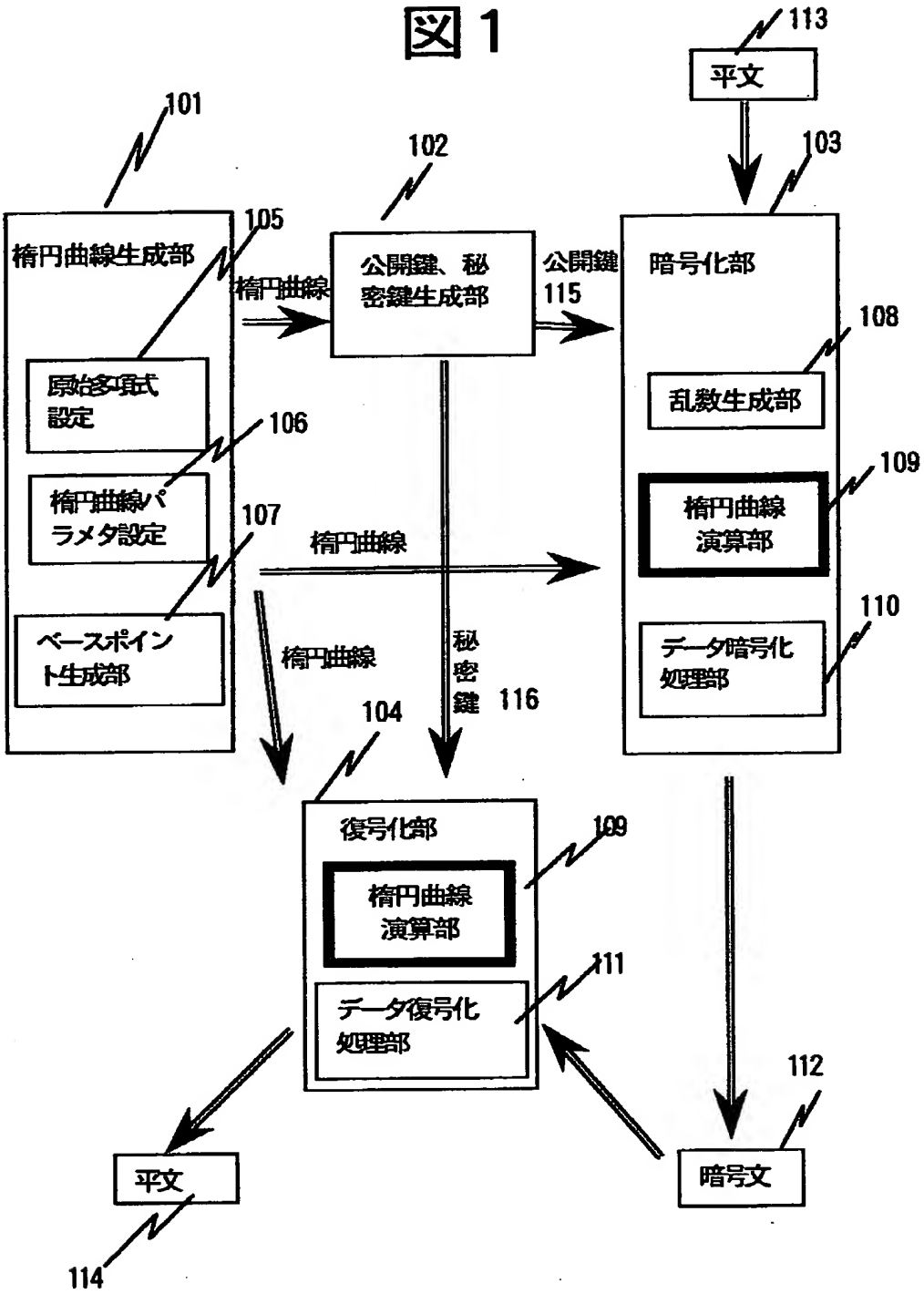
１１２　暗号文、

１１３　平文。

【書類名】　　図面

【図１】

図１


113
平文
101
102
103
105
楕円曲線生成部
楕円曲線
公開鍵、秘密鍵生成部
公開鍵
115
暗号化部
108
原始多項式設定
乱数生成部
106
楕円曲線パラメタ設定
109
楕円曲線演算部
107
楕円曲線
ベースポイント生成部
楕円曲線
秘密鍵
116
110
データ暗号化処理部
104
復号化部
109
楕円曲線演算部
111
データ復号化処理部
112
平文
暗号文
114

【図２】

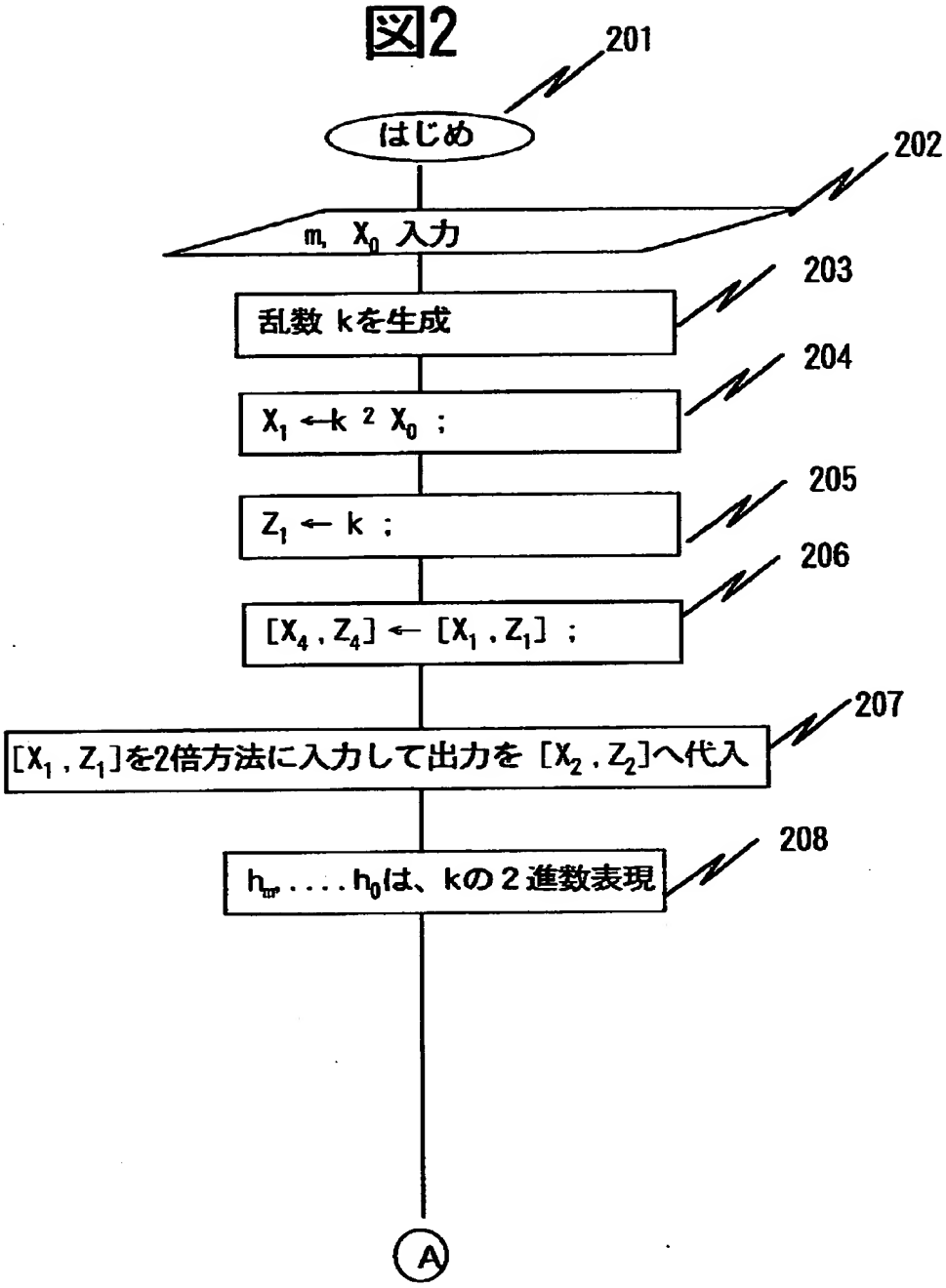
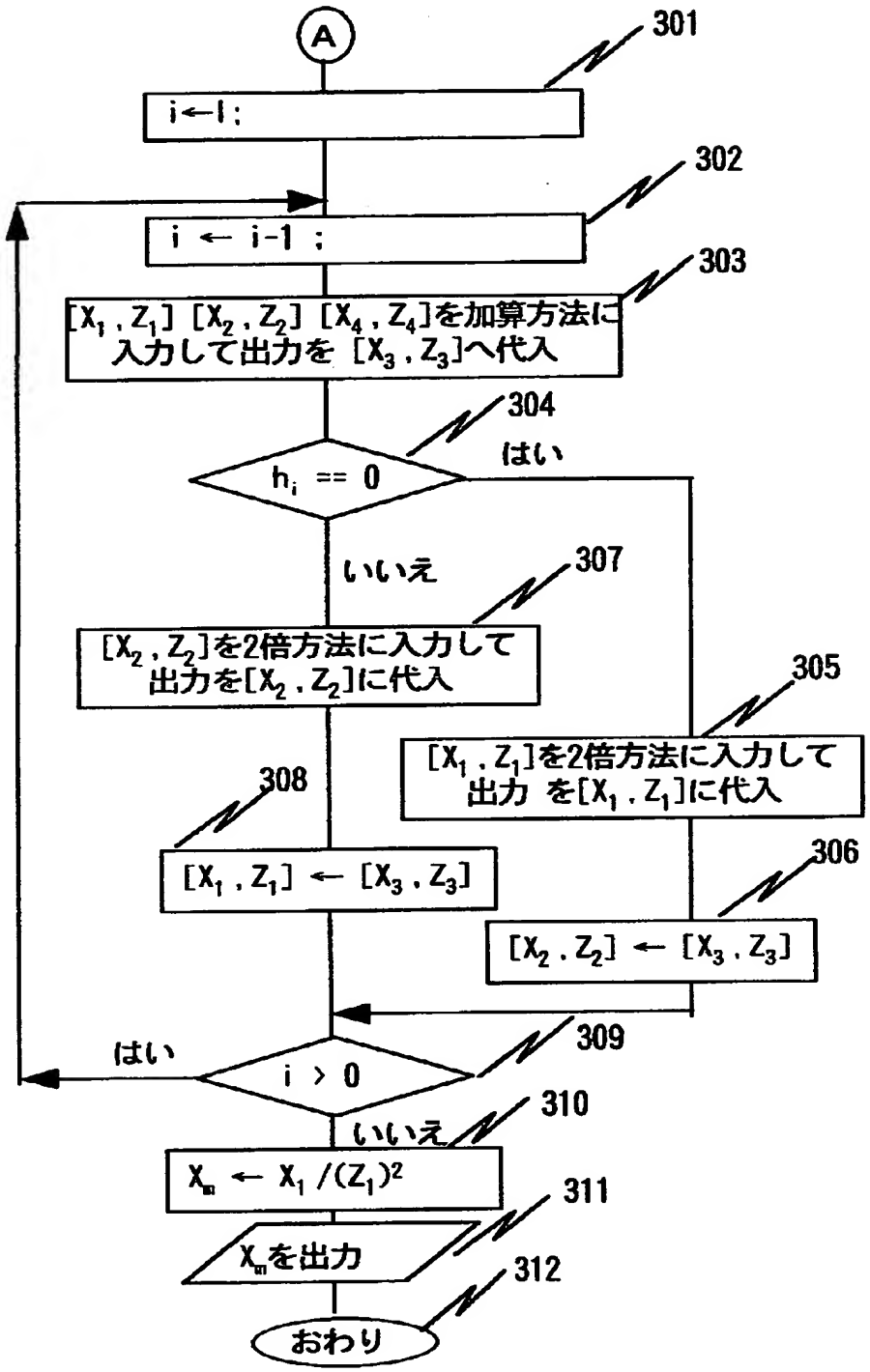


図2
201
はじめ
202
m, X0 入力
203
乱数 kを生成
204
X1 ←k 2 X0 ;
205
Z1 ← k ;
206
[X4 , Z4] ← [X1 , Z1] ;
207
[X1 , Z1]を2倍方法に入力して出力を [X2 , Z2]へ代入
208
hm .... h0は、kの２進数表現
A

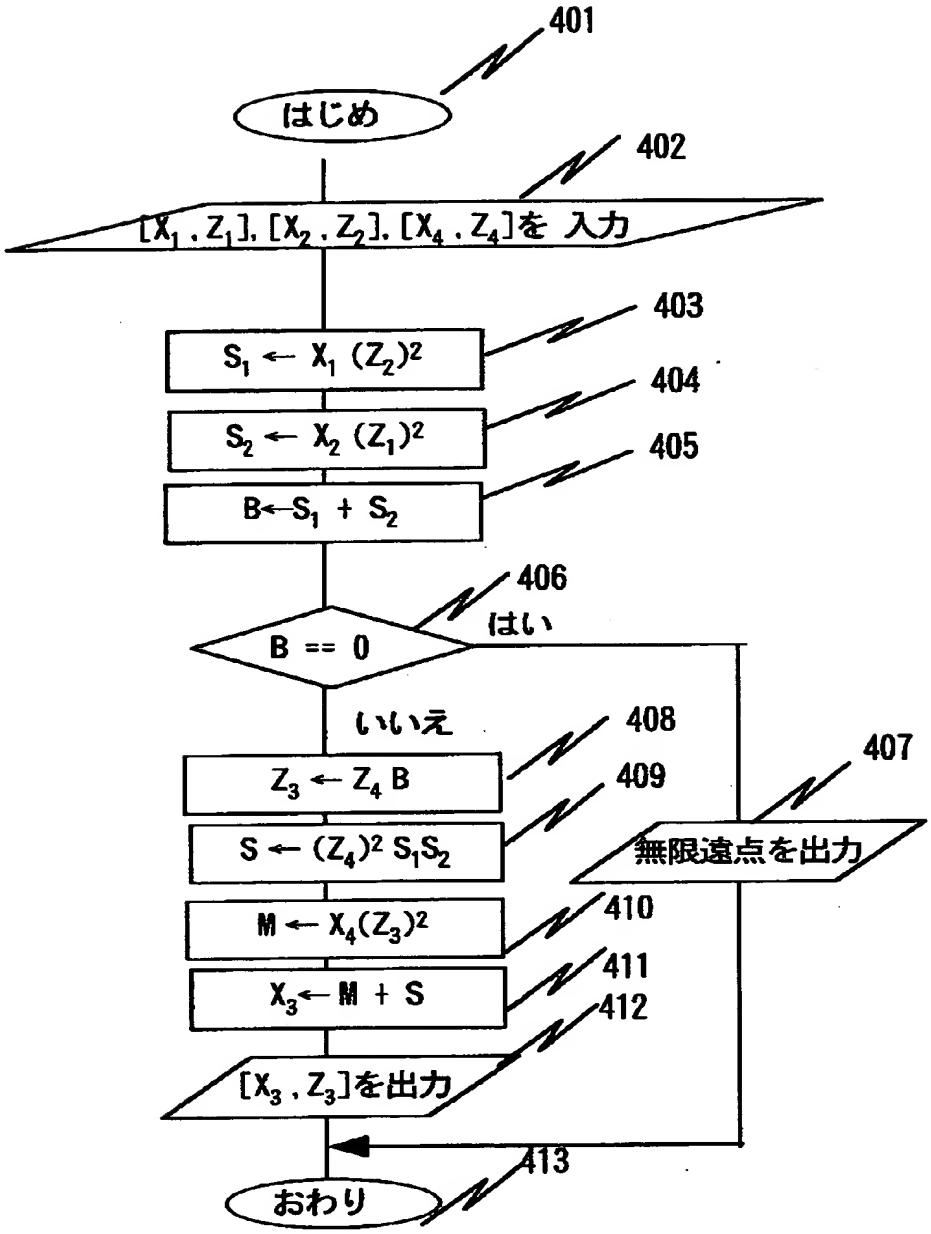
【図３】

図3


A
301
i←1;
302
i ← i-1 ;
303
[X1 , Z1] [X2 , Z2] [X4 , Z4]を加算方法に入力して出力を [X3 , Z3]へ代入
304
hi == 0
はい
いいえ
307
[X2 , Z2]を2倍方法に入力して出力を[X2 , Z2]に代入
305
[X1 , Z1]を2倍方法に入力して出力 を[X1 , Z1]に代入
308
[X1 , Z1] ← [X3 , Z3]
306
[X2 , Z2] ← [X3 , Z3]
309
はい
i > 0
310
いいえ
Xm ← X1 /(Z1)2
311
Xmを出力
312
おわり

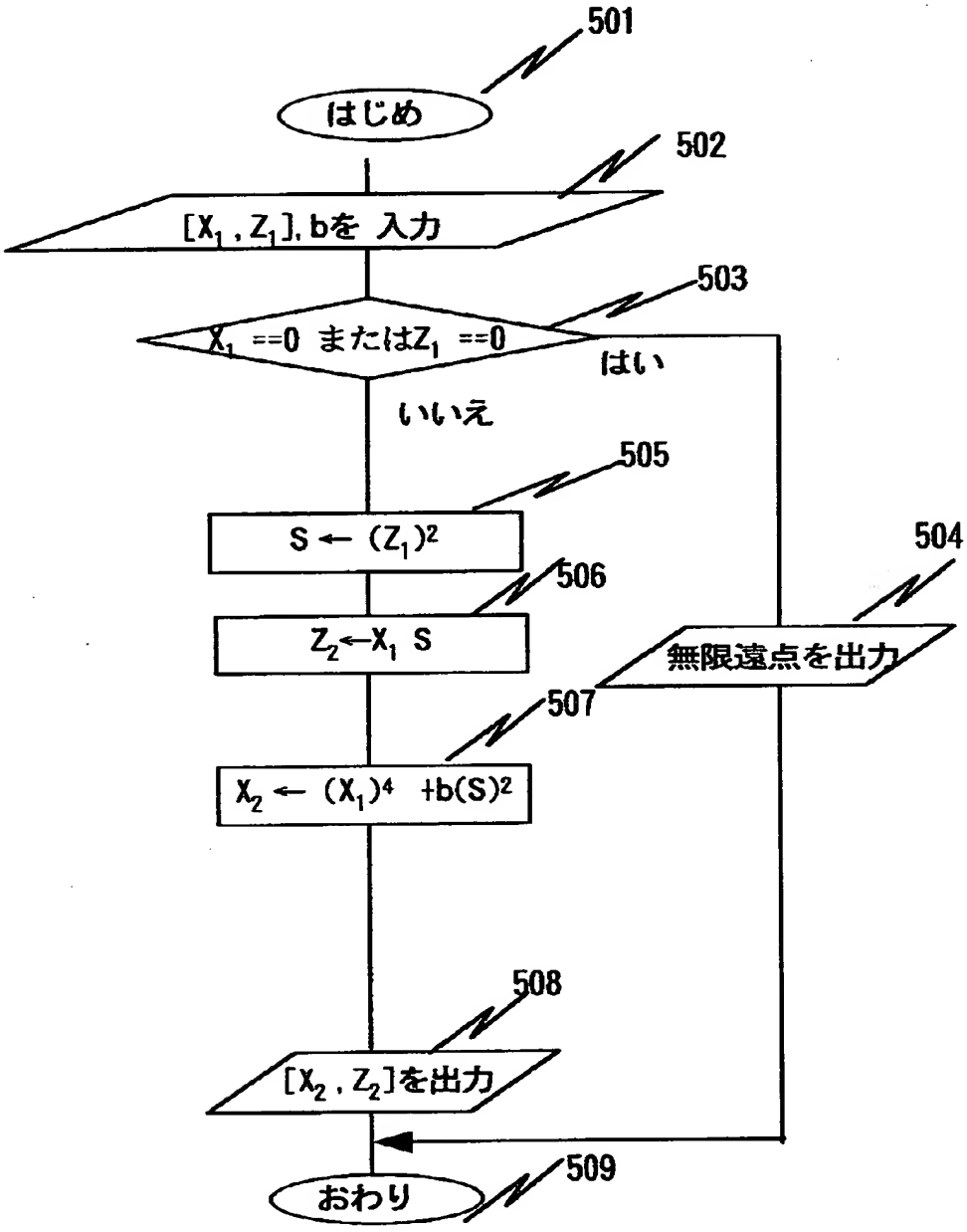
【図４】

図4


401
はじめ
402
[X1 , Z1], [X2 , Z2], [X4 , Z4]を 入力
403
S1 ← X1 (Z2)2
404
S2 ← X2 (Z1)2
405
B←S1 + S2
406
B == 0
はい
いいえ
407
無限遠点を出力
408
Z3 ← Z4 B
409
S ← (Z4)2 S1S2
410
M ← X4(Z3)2
411
X3←M + S
412
[X3 , Z3]を出力
413
おわり

【図５】

図5


501
はじめ
502
[X1 , Z1], bを 入力
503
X1 ==0 またはZ1 ==0
はい
いいえ
505
S ← (Z1)2
504
無限遠点を出力
506
Z2←X1 S
507
X2 ← (X1)4 +b(S)2
508
[X2 , Z2]を出力
509
おわり

【図６】

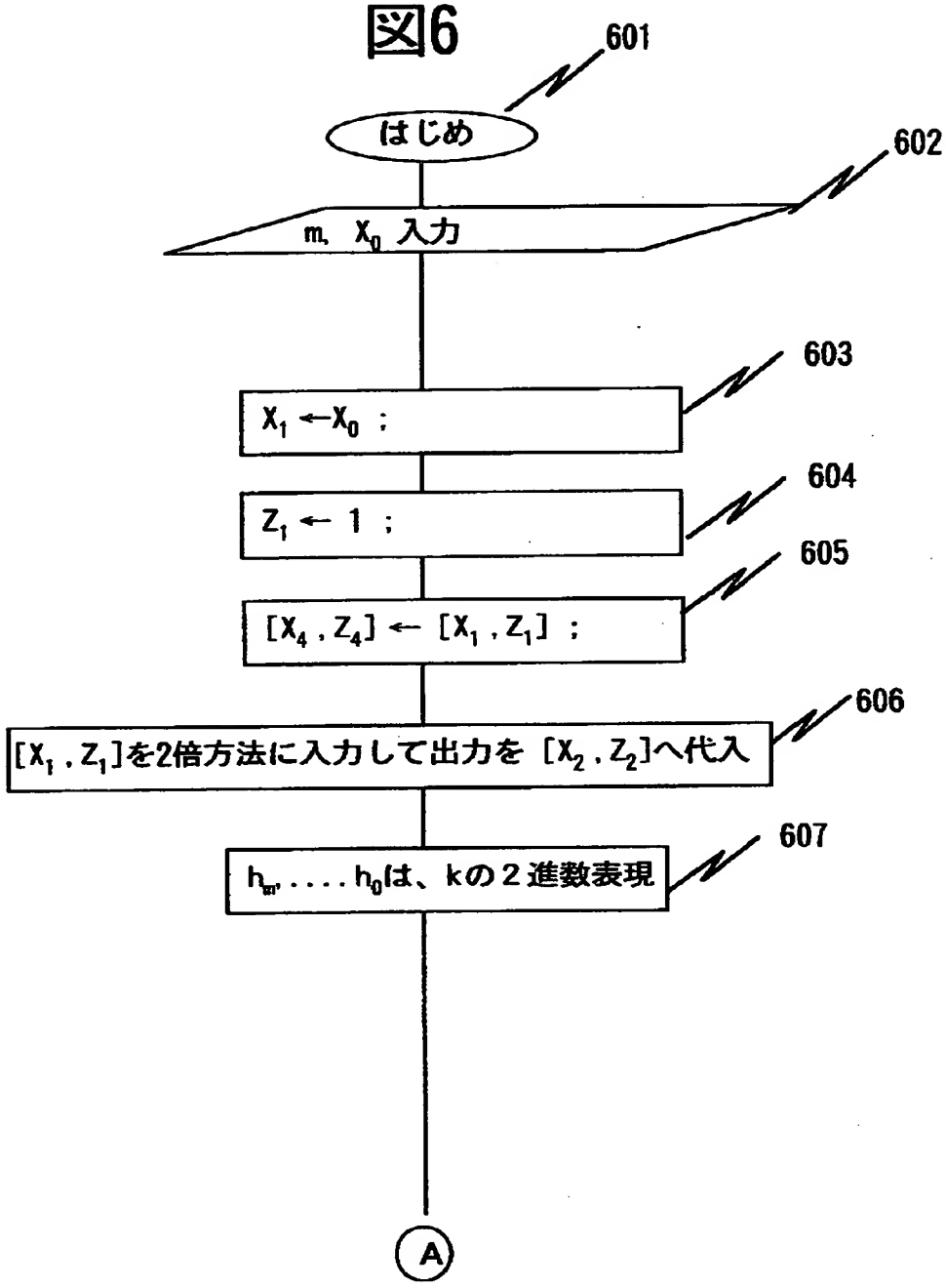
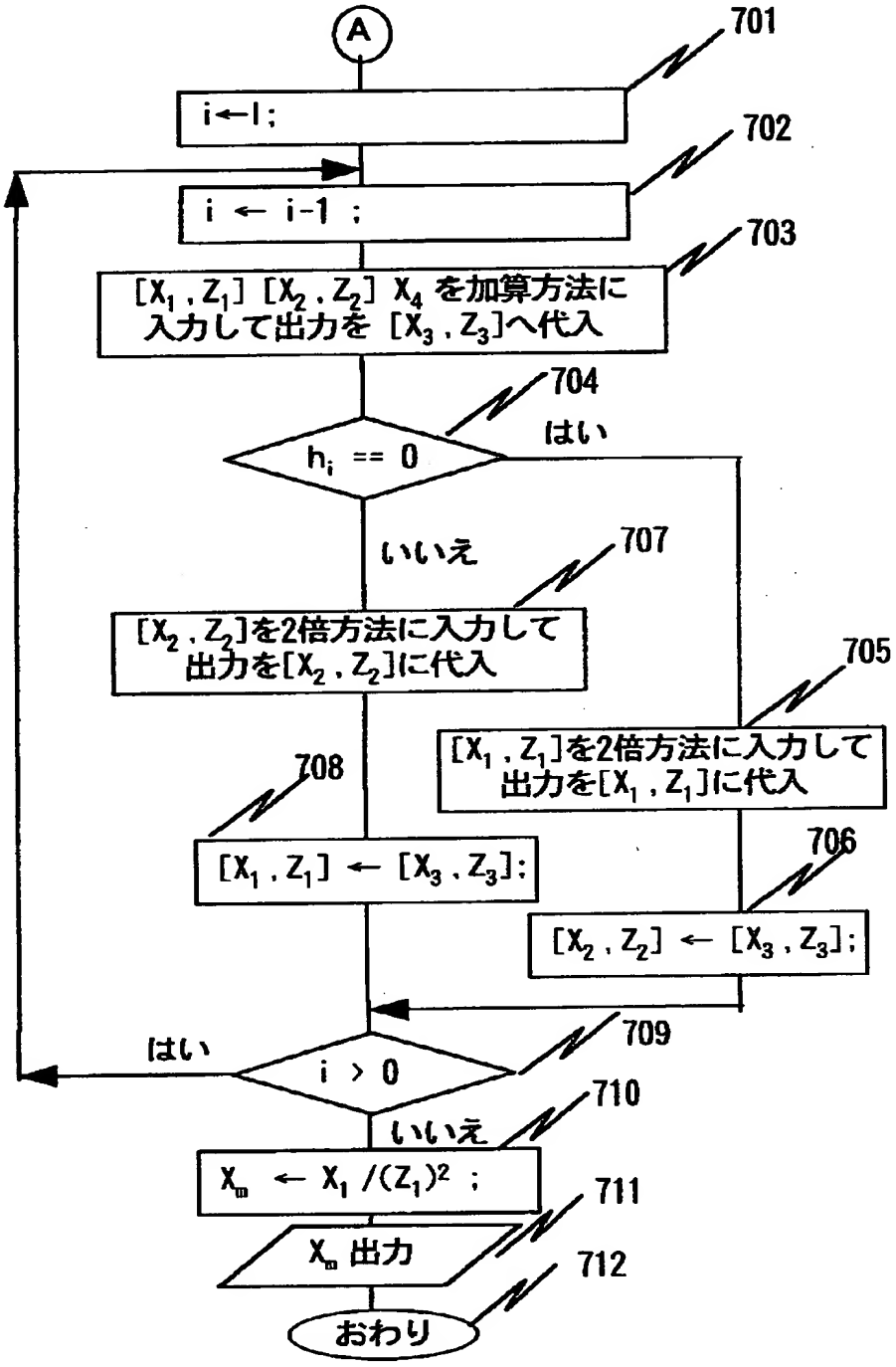


図6
601
はじめ
602
m, X0 入力
603
X1 ←X0 ;
604
Z1 ← 1 ;
605
[X4 , Z4] ← [X1 , Z1] ;
606
[X1 , Z1]を2倍方法に入力して出力を [X2 , Z2]へ代入
607
hm, ... h0は、kの２進数表現
A

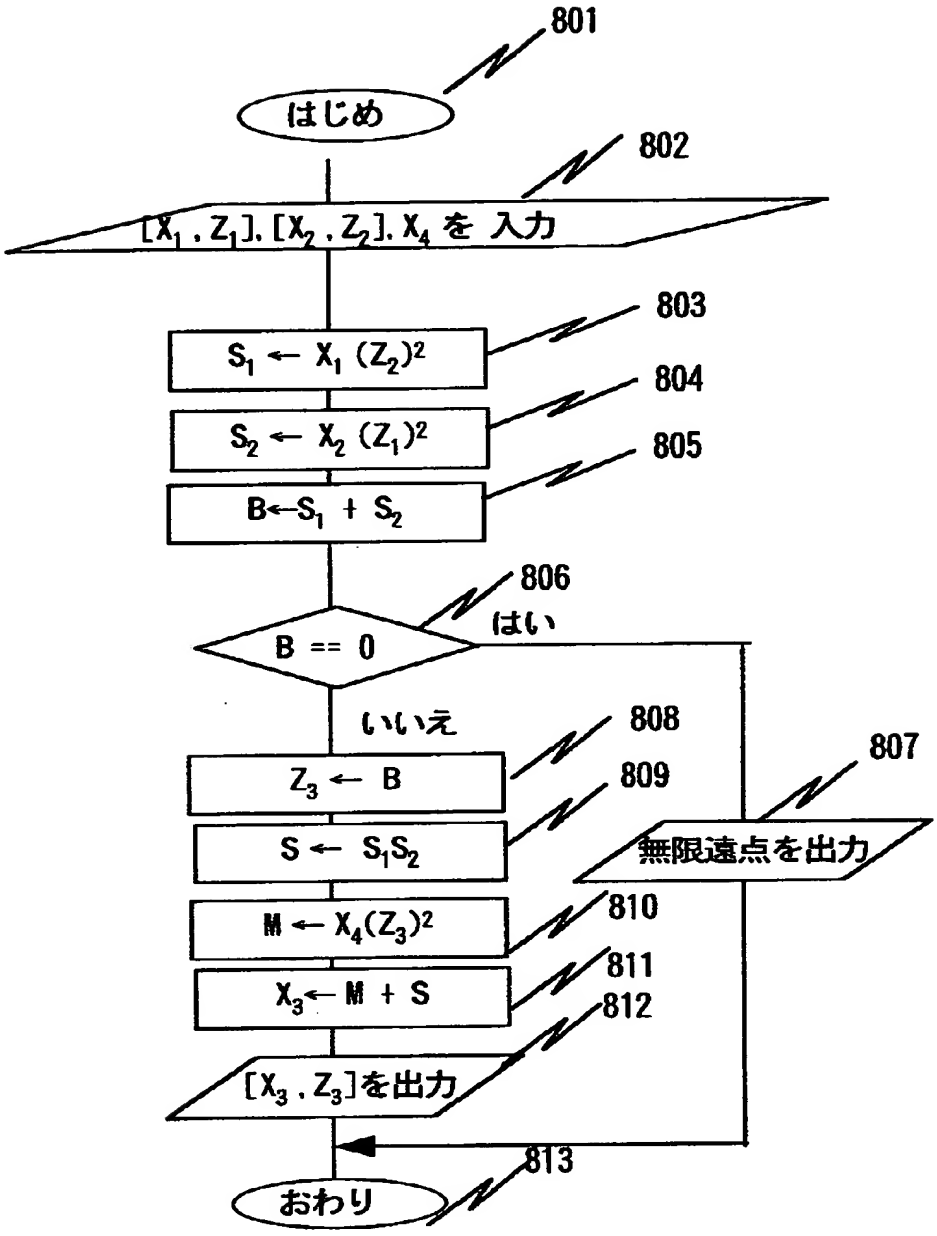
【図７】

図7


A
701
i←1;
702
i ← i-1 ;
703
[X1 , Z1] [X2 , Z2] X4 を加算方法に
入力して出力を [X3 , Z3]へ代入
704
hi == 0
はい
いいえ
707
[X2 , Z2]を2倍方法に入力して
出力を[X2 , Z2]に代入
705
[X1 , Z1]を2倍方法に入力して
出力を[X1 , Z1]に代入
708
[X1 , Z1] ← [X3 , Z3];
706
[X2 , Z2] ← [X3 , Z3];
はい
709
i > 0
710
いいえ
Xm ← X1 /(Z1)2 ;
711
Xm 出力
712
おわり

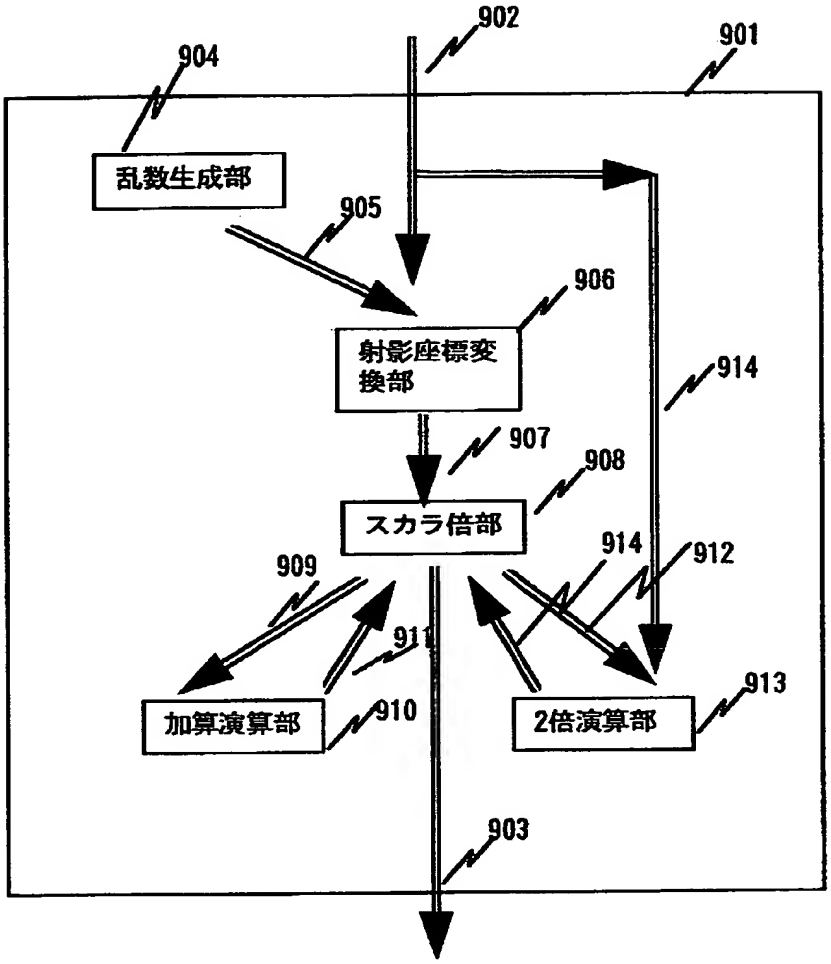
【図８】

図8


801
はじめ
802
[X1 , Z1], [X2 , Z2], X4 を 入力
803
S1 ← X1 (Z2)2
804
S2 ← X2 (Z1)2
805
B←S1 + S2
806
B == 0
はい
いいえ
807
無限遠点を出力
808
Z3 ← B
809
S ← S1S2
810
M ← X4(Z3)2
811
X3← M + S
812
[X3 , Z3]を出力
813
おわり

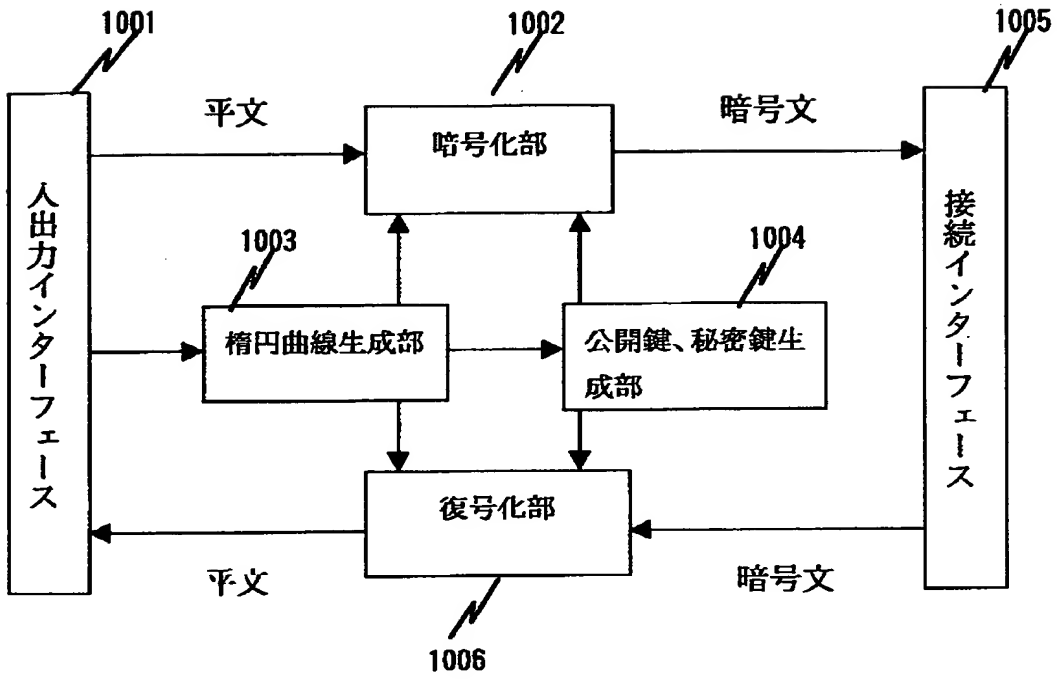
【図９】

図9


902
901
904
乱数生成部
905
906
射影座標変換部
914
907
908
スカラ倍部
914
912
909
911
加算演算部
910
2倍演算部
913
903

【図１０】

図１０


1001
1002
1005
平文
暗号文
暗号化部
人出力インターフェース
接続インターフェース
1003
1004
楕円曲線生成部
公開鍵、秘密鍵生成部
復号化部
平文
暗号文
1006

【書類名】　要約書

【要約】

【課題】

楕円曲線暗号処理を実行する方法は知られていたが、楕円曲線暗号のデータ復号化処理では、与えられた楕円曲線上の点（ｘ，ｙ）の秘密鍵ｄから、（ｘ，ｙ）のスカラー倍演算ｄ（ｘ，ｙ）を行う。　ｄの偏差情報をもれないスカラー倍演算方法で高速な方法を与える。

【解決手段】

次の手段を用いる。

（１）ｄのビットあたり一定の乗算回数でスカラー倍演算ｄ（ｘ，ｙ）を求める方法を与える。

（２）スカラー倍ｄ（ｘ，ｙ）を計算する場合、このアフィン座標（ｘ，ｙ）を射影座標する際に、乱数ｋを生成し、（ｘ，ｙ）→［ｋｘ，　ｋｙ，　ｋ］または（ｘ，ｙ）→［k^2ｘ，　k^3ｙ，　ｋ］に変換する。このことにより、素体の演算対象が乱数によって変更する方法を与える。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所